MANUAL DE INSTALACIÓN

1 ÍNDICE

1 Índice 2
2 Objetivo de este manual 12
3 ¿Más información? 12
4 Introducción: ¿Qué es Evolution? 12
5 Arquitectura 13
6 Instalación del servidor Evolution 14
6.1 Dimensionamiento de los servidores 14
6.2 Requerimientos de software 15
6.3 Preparación del servidor Windows Server 15
6.3.1 Windows 2003 Server 15
6.3.2 Windows 2008 Server R2 16
6.3.3 Windows 2012 Server 17
6.4 Preparación del servidor SQL Server 20
6.4.1 Acerca de MS SQL Server 2005 20
6.4.2 MS SQL Server 2008 20
6.4.3 MS SQL Server 2012 22
6.4.4 Cómo comprobar el orden de intercalación del servidor SQL 25
6.4.5 Cómo comprobar el modo de autenticación del servidor SQL 26
6.4.6 Cómo comprobar el nombre completo de la instancia del servidor SQL 26
6.4.7 Cómo instalar las librerias cliente de MS SQL Server 26
6.4.8 Recomendaciones prácticas sobre la base de datos 27
6.4.9 Sobre las cuentas de Usuarios de Base de Datos 27
6.4.10 Cómo restaurar una base de datos EVOLUTIONDB 28
6.4.11 Procedimientos auxiliares para mantenimiento de índices 29
6.5 Enlace con el servidor CTI 29
6.6 Instalación del Servidor Evolution 30
6.7 Configuración de los parametros del servidor Evolution 33
6.8 Introducción de las licencias de Evolution 34

6.8.1 Proceso de Licencia 35
6.9 Como comprobar el correcto acceso a Manager 37
6.10 Como configurar los parámetros de Manager 37
6.10.1 Cómo configurar los parámetros de chat interno 39
6.11 Como configurar los parámetros de Developer-Service 39
6.12 Cómo desinstalar el Servidor 40
7 Instalacion del entorno de desarrollo Developer.NET 42
7.1 Requerimientos 42
7.2 Instalación de Developer.NET 42
8 Instalacion de la aplicación iAgent 45
8.1 Requerimientos 45
8.2 Instalación de la aplicación agente 45
8.3 Parametrización en registry 47
8.4 Soporte para terminal server 48
9 iAgentWebPortal: Despliegue Web de la aplicación de agente 49
9.1 Como configurar iAgent Web Portal 49
9.2 Como se accede a iAgent Web Portal 51
10 Instalación del servidor WebChat 53
10.1 Requerimientos 53
10.2 Instalación 53
10.3 Configuración de los parametros de WebChat 54
10.3.1 Configuración de web.config 54
10.3.2 Configuración por temas 55
10.4 Cómo iniciar una sesión con WebChat 55
10.5 Instalación de VideoChat 56
10.5.1 Instalación del servidor Red5 56
10.5.2 Configuración de VideoChat 57
10.5.3 Verificación de VideoChat 57
10.6 Securización de las comunicaciones WebChat 58
10.6.1 Verificación de integridad de la URL 58

10.6.2 Publicación HTTPS 58
11 Task Daemon 59
11.1 Como modificar la configuración del servicio Task Daemon 59
11.1.1 Comunicación con EvoServer y configuración del servicio 59
11.1.2 Mantenimiento de la base de datos 59
12 Dynamic Business Router 61
12.1 Evorouter Daemon 61
12.2 Parámetros del servicio 61
12.2.1 Configuración del servicio 61
12.2.2 En interacciones interactivas, ¿Cómo configurar EvoRouter para que seleccione la estrategia por defecto a partir del DN del RoutePoint? 62
12.2.3 Instalación de Voces adicionales para funcionalidades de sintesis de voz y reconocimiento del habla. 62
13 Developer Service 63
14 Módulo Grabador 64
14.1 Esquema Generico 64
14.1.1 Grabador ICR (Recorder Daemon) 64
14.1.2 Grabador Asterisk 65
14.2 Requerimientos Capacidad de Almacenamiento 65
14.3 Alta de una instancia de Grabador en Manager 66
14.4 Notas Técnicas Grabador ICR 67
14.4.1 Proceso de Instalación Manual de iAgent: 67
14.4.2 Proceso de Instalación Manual del Módulo Servidor 67
14.4.3 Envío de grabaciones off-line 67
14.4.4 Parámetros del DaemonRecorder (módulo Servidor) 67
14.4.5 Parámetros del módulo MGC (agente) 68
14.5 Notas Técnicas Grabador Asterisk 68
14.5.1 Requisitos en el servidor evolution 68
14.5.2 Proceso de instalación scripts para asterisk como servicio 68
14.5.3 Descripción de los scripts para asterisk 69
14.5.4 Otros usos de los scripts para asterisk 71

14.6 Notas Técnicas Grabador NICE 71
14.6.1 Configuración certificada 71
14.6.2 Archivo de configuración 71
14.6.3 Conexión al servicio web 72
14.6.4 Mapeado de los datos de negocio 72
14.7 Configuración del número de threads por grabador 73
15 Securización de las comunicaciones 74
15.1 ¿Cómo publicar una aplicación vía HTTPS en IIS? 74
15.2 Manager 77
15.2.1 Grabación integrada Asterisk / SIP Call Manager 79
15.3 Securización del acceso iAgent mediante SSL (stunnel) 79
15.3.1 ¿Que es stunnel? 79
15.3.2 Cómo instalar stunnel en el servidor Evolution 79
15.3.3 Notas adicionales sobre la seguridad 82
15.4 Argumentarios y páginas de sistema de Evolution 82
15.5 Securización del despliegue con Developer.NET 82
15.6 WebChat 84
16 ANEXO A: Configuraciones de telefonía 87
16.1 Avaya Aura Communications Manager y AES 87
16.1.1 Configuración certificada 87
16.1.2 Cómo configurar el servidor TSAPI AES 87
16.1.3 Cómo Instalar el cliente TSAPI AES 91
16.1.4 Cómo comprobar el correcto funcionamiento de TSAPI AES 92
16.1.5 Cómo configurar el enlace Evolution al servidor TSAPI AES 92
16.1.6 Cómo configurar el módulo ICR Dialer Daemon (EvoDialerServer) 93
16.1.7 Cómo administrar los dispositivos de marcación en Evoadmin 94
16.1.8 Configuraciones de Evolution Manager 95
16.1.9 Notas técnicas 98
16.2 Avaya IP Office 99
16.2.1 Configuración certificada 99

16.2.2 ¿Cómo gestiona Evolution las extensiones de los agentes? 99
16.2.3 Cómo configurar el servidor AVAYA IP OFFICE 99
16.2.4 Cómo Instalar el cliente IPOFFICE TAPI3 (TAPI SERVICE PROVIDER) 104
16.2.5 Cómo comprobar el correcto funcionamiento de IPOFFICE TAPI SERVICE PROVIDER 105
16.2.6 ¿Qué hacer si no aparecen las extensiones recientemente configuradas? 105
16.2.7 Cómo configurar el enlace Evolution al servidor IPOFFICE AVAYA 105
16.2.8 Cómo configurar el módulo ICR Dialer Daemon (EvoDialerServer) 107
16.2.9 Cómo administrar los dispositivos de marcación en Evoadmin 108
16.2.10 Configuraciones de Evolution Manager 109
16.2.11 Limitaciones conocidas de Evolution con Avaya IP Office 110
16.3 Avaya CS1000 & CC7 112
16.3.1 Cómo configurar el servidor CTConnect server 112
16.3.2 Cómo Instalar el Cliente Syntellect CT Connect client 113
16.3.3 Cómo configurar el enlace Evolution al servidor NORTEL CC7 113
16.3.4 Cómo configurar el módulo ICR Dialer Daemon (EvoDialerServer) 114
16.3.5 Cómo administrar los dispositivos de marcación en Evoadmin 115
16.3.6 Configuraciones de Evolution Manager 116
16.4 Nortel Meridian-1 & Symposium 5/6 118
16.4.1 Cómo configurar el servidor CTConnect server 118
16.4.2 Cómo Instalar el Cliente Syntellect CT Connect client 119
16.4.3 Cómo configurar el enlace Evolution al servisor Symposium 120
16.4.4 Cómo configurar el módulo ICR Dialer Daemon (EvoDialerServer) 121
16.4.5 Cómo administrar los dispositivos de marcación en Evoadmin 121
16.4.6 Configuraciones de Evolution Manager 122
16.5 CISCO Communications Manager CM/UCM 125
16.5.1 Configuración certificada 125
16.5.2 Cómo administrar un usuario Cisco para Evolution 125
16.5.3 Cómo asociar las líneas de los teléfonos al usuario Evolution 126
16.5.4 Cómo configurar los dispositivos CTI Route Point necesarios 126
16.5.5 Cómo administrar rutas de llamadas entrantes en Cisco CM 127

16.5.6 Cómo configurar los dispositivos CTI Ports necesarios 127
16.5.7 Cómo instalar los componentes CiscoTSP y Cisco Wave Driver 128
16.5.8 Cómo comprobar el correcto funcionamiento de CiscoTSP 129
16.5.9 Cómo configurar el enlace Evolution al CISCO TAPI 130
16.5.10 Cómo configurar los dispositivos de marcacion en evoadmin 131
16.5.11 Cómo configurar el módulo ICR Dialer Daemon (EvoDialerServer) 131
16.5.12 Cómo configurar usuarios y puestos en Evolution Manager 132
16.5.13 Cómo configurar campañas DBR en Evolution Manager 132
16.6 Panasonic serie TDA/TDE 134
16.6.1 Cómo Instalar el Cliente PANASONIC KX-TDA TAPI SERVICE PROVIDER 134
16.6.2 Cómo configurar el enlace Evolution a PANASONIC KX-TDA TSP 135
16.6.3 Configuraciones de Evolution Manager 136
16.6.4 Notas técnicas 137
16.7 Alcatel Omni PCX Enterprise, ALCATEL 4400 140
16.7.1 Cómo configurar el servidor CTConnect server 140
16.7.2 Cómo Instalar el Cliente Syntellect CT Connect client 141
16.7.3 Cómo configurar el enlace Evolution al switch OmniPCX 141
16.7.4 Cómo configurar el módulo ICR Dialer Daemon (EvoDialerServer) 142
16.7.5 Configuraciones de Evolution Manager 143
16.7.6 Notas técnicas 144
16.8 IP-PBX Asterisk 145
16.8.1 Configuración certificada 145
16.8.2 Cómo habilitar la interfaz de conexión AMI en Asterisk 146
16.8.3 Cómo configurar las extensiones 147
16.8.4 Cómo configurar las colas ACD Asterisk 148
16.8.5 Cómo configurar una extensión tipo Route-Point 149
16.8.6 Ejemplo de un fragmento de dial plan mínimo 150
16.8.7 Cómo instalar ActivaTSP (TAPI Service Provider) 151
16.8.8 Cómo comprobar el correcto funcionamiento del conjunto ActivaTSP / Asterisk 152
16.8.9 Cómo configurar el enlace Evolution al servidor Asterisk 153

16.8.10 Cómo configurar el módulo ICR Dialer Daemon (EvoDialerServer) 154
16.8.11 Cómo administrar los dispositivos de marcación en Evoadmin 155
16.8.12 Cómo configurar usuarios y puestos en Evolution Manager 156
16.8.13 Cómo configurar campañas switch-based en Evolution Manager 156
16.8.14 Cómo configurar developer service para subir locuciones asociadas a LOS SCRIPTS DBR 159
16.8.15 Cómo configurar campañas DBR en Evolution Manager 159
16.8.16 Cómo configurar Manager para supervisar conversaciones 161
16.8.17 Notas técnicas 162
16.9 IP-PBX Asterisk ELASTIX 162
16.9.1 Configuración certificada 163
16.9.2 Cómo crear las extensiones Elastix 164
16.9.3 Cómo crear las colas ACD Elastix 164
16.9.4 Cómo configurar una extensión tipo Route-Point 165
16.9.5 Cómo habilitar la interfaz de conexión AMI en Asterisk 166
16.9.6 Cómo instalar ActivaTSP (TAPI Service Provider) 167
16.9.7 Cómo comprobar el correcto funcionamiento del conjunto ActivaTSP / Asterisk 168
16.9.8 Cómo configurar el enlace Evolution al servidor Asterisk 168
16.9.9 Cómo configurar el módulo ICR Dialer Daemon (EvoDialerServer) 169
16.9.10 Cómo administrar los dispositivos de marcación en Evoadmin 170
16.9.11 Cómo configurar usuarios y puestos en Evolution Manager 171
16.9.12 Cómo configurar campañas switch-based en Evolution Manager 172
16.9.13 Cómo configurar developer service para subir locuciones asociadas a LOS SCRIPTS DBR 173
16.9.14 Cómo configurar campañas DBR en Evolution Manager 174
16.9.15 Notas técnicas 176
17 ANEXO B: Instalación de mediaserver para soporte DBR 178
17.1 Cómo instalar un MediaServer basado en Elastix 178
17.1.1 Configuración certificada 178
17.1.2 Instalación de ELASTIX 178
17.1.3 Recomendaciones sobre la conexión LAN entre Evolution Server y Media Server. 179

17.1.4 ¿Cómo configurar una extensión SIP para pruebas en MediaServer? 179
17.1.5 ¿Cómo revisar el modo-compatibilidad CompatResAGIVersion=1.4 de ELASTIX? 180
17.1.6 Cómo configurar una extensión tipo Route-Point 180
17.1.7 Cómo agregar las extensiones Route-point al módulo “Misc. Destinations” 181
17.1.8 Cómo configurar un enlace SIP para las llamadas inbound (trunk SIP) 182
17.1.9 Cómo configurar las rutas de llamadas inbound 182
17.1.10 Cómo configurar las rutas de llamadas outbound 183
17.1.11 Cómo comprobar el trunk SIP y las rutas inbound/outbound 184
17.1.12 Cómo habilitar la interfaz de conexión AMI 184
17.1.13 Cómo instalar ActivaTSP (TAPI Service Provider) 185
17.1.14 Cómo comprobar el correcto funcionamiento del conjunto ActivaTSP / Asterisk 186
17.1.15 Cómo configurar el modo ‘MediaGateway’ en Evoserver 186
17.1.16 Cómo configurar el módulo ICR Dialer Daemon (EvoDialerServer) 187
17.1.17 Cómo configurar campañas DBR en Evolution Manager 187
17.2 Cómo instalar un MediaServer basado en Asterisk 189
17.2.1 Configuración certificada 189
17.2.2 Instalación de Asterisk en RedHad/Centos 190
17.2.3 Recomendaciones sobre la conexión LAN entre Evolution Server y Media Server. 192
17.2.4 ¿Cómo configurar una extensión SIP para pruebas en MediaServer? 192
17.2.5 ¿Cómo revisar el modo-compatibilidad CompatResAGIVersion=1.4 de Asterisk? 193
17.2.6 Configuración para que el destino de cualquier llamada entrante por el trunk se considere Route-Point 193
17.2.7 Cómo configurar un enlace SIP para las llamadas inbound (trunk SIP) 194
17.2.8 Cómo configurar las rutas de llamadas “outbound” 195
17.2.9 Cómo comprobar el trunk SIP y las rutas inbound/outbound 195
17.2.10 Cómo habilitar la interfaz de conexión AMI 196
17.2.11 Cómo instalar ActivaTSP (TAPI Service Provider) 197
17.2.12 Cómo comprobar el correcto funcionamiento del conjunto ActivaTSP / Asterisk 198
17.2.13 Cómo configurar el modo ‘MediaGateway’ en Evoserver 199
17.2.14 Cómo configurar el módulo ICR Dialer Daemon (EvoDialerServer) 199

17.2.15 Cómo configurar campañas DBR en Evolution Manager 200
17.2.16 Cómo configurar Developer Service para que despliegue los audios en el Media Server 202
17.3 Configuración específica para CISCO Communications Manager CM/UCM 203
17.3.1 Configuración certificada 203
17.3.2 Cómo configurar los elementos CTI específicos para CISCO 203
17.3.3 Configurar trunk sip en Cisco 204
17.4 Configuración para AVAYA AURA Communications Manager 205
17.4.1 Configurar trunk sip en AVAYA CM 205
17.4.2 Configurar SIP Call Manager 205
18 ANEXO C: Configuración de conectores DBR no interactivos 206
18.1 Conector DBR POP3/POP3S 206
18.1.1 Prerequisitos 206
18.1.1 Cómo configurar el conector POP3/POP3S en Evolution Manager 206
18.2 Conector DBR email IMAP(S) 207
18.2.1 Prerequisitos 207
18.2.2 Parámetros IMAP 208
18.2.3 Cómo configurar el conector IMAP(S) en Evolution Manager 209
18.3 Conector DBR WebService API 211
18.3.1 Cómo configurar el conector WebService API en Evolution Manager 211
18.4 Conector DBR Twitter 213
18.4.1 Prerequisitos 213
18.4.2 Cómo configurar un conector Twitter en Evolution Manager 213
18.4.3 Notas técnicas 216
18.5 Como codificar caracteres especiales en las definiciones de conectores (URL) 217
19 ANEXO D: Instalación en un 'cluster failover' de Windows 2008 219
19.1 Requerimientos 219
19.2 Instalación del servidor Evolution 219
19.3 Configuración del 'Servicio de alta disponibilidad de Evolution' 220
19.4 Configuración compartida de los IIS 222

2 OBJETIVO DE ESTE MANUAL

Este manual describe los procedimientos para la instalación de los módulos de Evolution, así como las operaciones normalmente utilizadas en su configuración y administración.

3 ¿MÁS INFORMACIÓN?

Para obtener más información acerca de Evolution, entre al Centro de Recursos en http://www.evolutioncallcenter.com, donde encontrará más tutoriales, manuales, y el foro de acceso público de Evolution.

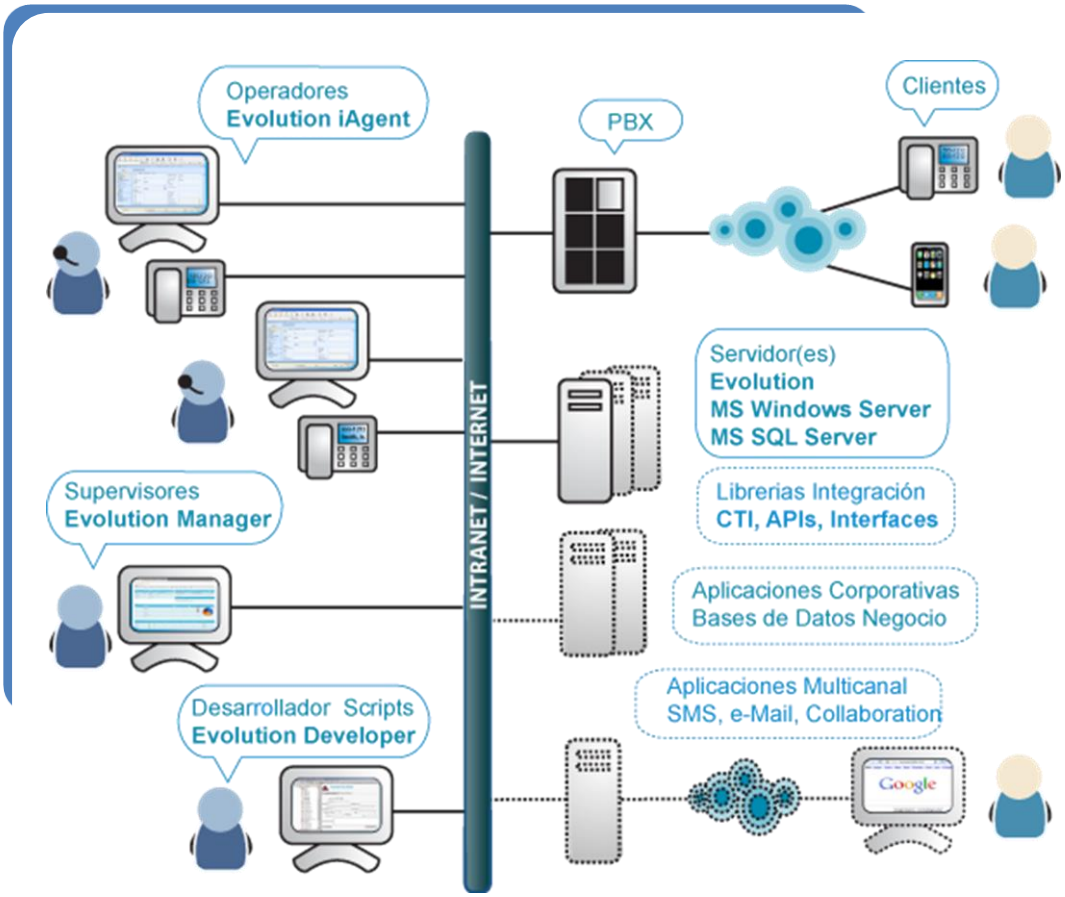
4 INTRODUCCIÓN: ¿QUÉ ES EVOLUTION?

Evolution es la solución de software para call centers basada en web que cubre las necesidades de contactos entrantes y salientes, al tiempo que sus Módulos de Supervisión, Administración e Informes, ayudan a gestionar y cuantificar el rendimiento del call center. Permite desarrollar argumentarios en múltiples modalidades, integrándolos con el interfaz utilizado por los agentes.

Incorpora conectores y potentes APIs que facilitan la integración de aplicaciones y canales alternativos de comunicación, adaptándose ágilmente a las tecnologías y requerimientos de la empresa.

5 ARQUITECTURA

Evolution consta de varios módulos:



- Servidor Evolution: Se comunica con la centralita PBX y con la base de datos SQL, y constituye el verdadero corazón del call center Evolution.
- Agentes Evolution, instalados en los PC de los teleoperadores, proporcionan las herramientas necesarias para su operativa.
- Manager Evolution permite que los supervisores controlen y administren el funcionamiento de las campañas y servicios.
- Developer.NET es la herramienta con la que los desarrolladores pueden construir argumentarios y aplicaciones Evolution.
- Centralita PBX compatible. En la actualidad Evolution es compatible con las principales centralitas del mercado como Avaya, Nortel, Alcatel, Panasonic y otras, incluyendo la centralita de código abierto Asterisk.
- Base de Datos SQL: En la actualidad Evolution gestiona sus datos con MS SQL Server 2005 o MS SQL Server 2008. En el futuro se incorporarán otras bases de datos.

6 INSTALACIÓN DEL SERVIDOR EVOLUTION

Este manual refiere a la versión Evolution versión 10

Se recomienda seguir los siguientes pasos para instalar o actualizar **Evolution/Server**

1. Si desea actualizar un servidor **Evolution/server** previamente instalado, recomendamos realice copias de seguridad de la base de datos, de los archivos de la versión anterior y de registry Windows bajo `hk_lm/software/icr`.
2. Revise los requerimientos previos. Instale y configure Software Base Requerido.
3. Instale el software **Evolution/server**
4. Configuración de **Evolution/server**.

6.1 DIMENSIONAMIENTO DE LOS SERVIDORES

El uso de recursos de los servidores está en función de la operativa y uso reales del sistema, por lo que solamente puede determinarse tras un estudio detallado de los requerimienstos funcionales y técnicos de cada proyecto.

Para consultas acerca del dimensionamiento y características de los servidores para un proyecto determinado, consultar con ICR.

A continuación se muestra una **tabla orientativa para el dimensionamiento de servidores:**

Escenario	Servidor
50 AGENTES, INBOUND&OUTBOUND, PREDICTIVE DIALING	EVOLUTION SERVER & DATABASE: 1 CPU x4 CORE Intel Xeon 3,2 GHz, 4 GB RAM, 200 GB
125 AGENTES, INBOUND&OUTBOUND, PREDICTIVE DIALING	EVOLUTION SERVER: 1 CPU x4 CORE Intel Xeon 3,2 GHz, 4 GB RAM, 200 GB DATABASE: 1 CPU x 4 CORE Intel Xeon 3,2 GHz, 6 GB RAM, RAID-5 de 200
200 AGENTES, INBOUND	EVOLUTION SERVER: 1 CPU x 4 CORE Intel Xeon 3,2 GHz, 4 GB RAM, 200 GB DATABASE: 1 CPU x 4 CORE Intel Xeon 3,2 GHz, 6 GB RAM, RAID-5 de 200

El espacio necesario en base de datos varía en función del número de registros de clientes y del número de registros de transacciones que se deseen mantener en las tablas de históricos.

Si se utilizan módulos de grabación de llamadas también deberá preverse el espacio necesario para almacenar los ficheros de audio correspondientes a las grabaciones. El espacio ocupado dependerá del formato de compresión escogido.

6.2 REQUERIMIENTOS DE SOFTWARE

Para instalar y ejecutar **Evolution Server** se requiere el siguiente software:

Software	Requerimiento
S.O.	Microsoft© Windows 2003 R2 Microsoft© Windows 2008 (32 bits) Microsoft© Windows 2008 R2 (64 bits) Microsoft© Windows 2012 (64 bits) Microsoft© Windows 2012 R2 (64 bits)
SGBD	MS SQL-SERVER 2005 o 2005 Express Edition MS SQL-SERVER 2008 o 2008 Express Edition MS SQL-SERVER 2008 R2 o 2008 R2 Express Edition MS-SQL-SERVER 2012 o 2012 Express Edition
Servidor WEB	MS IIS con ASP.NET instalado
Cliente CTI	Ver "16 ANEXO A: Configuraciones de telefonía"

6.3 PREPARACIÓN DEL SERVIDOR WINDOWS SERVER

La aplicación Manager Evolution y los argumentarios/aplicaciones generados con Developer.NET Evolution se ejecutan en un servidor web Microsoft Internet Information Server

6.3.1 WINDOWS 2003 SERVER

La aplicación Manager Evolution y los argumentarios/aplicaciones generados con Developer.NET Evolution se ejecutan en un servidor web Microsoft Internet Information Server.

Instalación y configuración del servidor Microsoft Internet Information Server

1 Compruebe que el servidor en el que desea instalar Evolution tiene instalado y configurado el Microsoft Internet Information Server (IIS) y los componentes necesarios:

- ASP (classic)
- ASP.NET
- Server Side Includes
- IIS services Management

Panel de control | Agregar o quitar programs, Seleccionar "Agregar o quitar components de Windows", Seleccionar "Servidor de aplicaciones", pulsar Detalles y seleccionar "ASP.NET". Seleccionar "Instalar Internet Information Services (IIS)", pulsar Detalles y seleccionar "Administrador de servicios de Internet Information Server", "Archivos comunes", "Servicio World Wide Web". Dentro de este último, seleccionar los subcomponentes "Páginas Active Server"

"Inclusiones de servidor" y "Servicio World Wide Web"

Puede comprobarse en Herramientas administrativas | Administrador de Internet Information Services (IIS), seleccionar "Extensiones de Servicio Web"

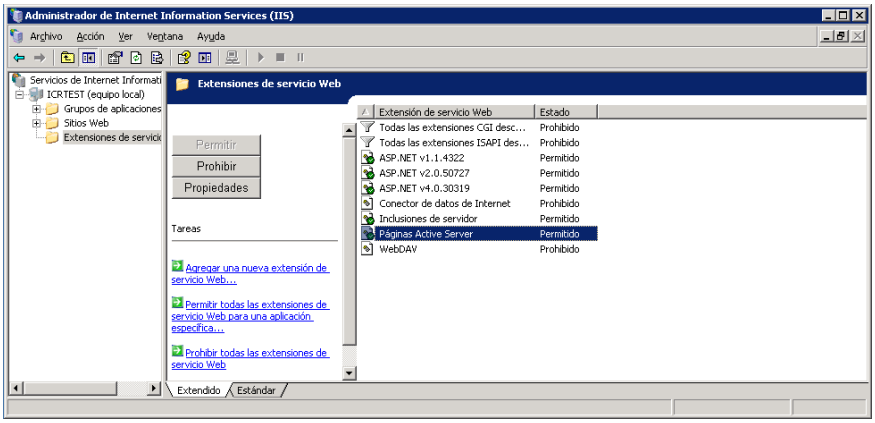
2 Una vez completada la instalación de IIS ASP.NET instale Microsoft Framework .NET v4 (.NET FW4).

La instalación de .NET FW4 modifica la configuración de IIS ASP.NET registrando el entorno **ASP.NET v4**.

Por ello es muy importante instalar .NET FW4 **despues** de haber completado previamente la instalación de ASP.NET.

Si instala ASP.NET después de instalar .NET FW4 es posible que el entorno ASP.NET v4 no quede correctamente configurado.

3 Compruebe que el entono ASP.NET ha quedado bien configurado.



6.3.2 WINDOWS 2008 SERVER R2

Instalación y configuración del servidor Microsoft Internet Information Server

1 Compruebe que el servidor en el que desea instalar Evolution tiene instalado y configurado el Microsoft Internet Information Server (IIS) y los componentes necesarios:

- ASP (classic)
- ASP.NET
- Server Side Includes
- IIS 6 Management Compatibility

1- Control panel | Programs, Seleccionar “Turn Windows features on or off”, Seleccionar “roles”, “add roles”. En “server roles”, seleccionar “Web Server (IIS)”, Siguiente, Siguiente
2- Seleccionar los siguientes “role services to install for Web Server (IIS)”:
   - Web Server | Application Development: **ASP.NET** (marca automáticamente otras dependencias), **ASP, Server Side Includes**
   - Web Server | Management tools: **IIS 6 Management Compatibility (seleccionar todas)**
3- Siguiente, instalar

2 Una vez completada la instalación de IIS ASP.NET instale Microsoft Framework .NET v4 (.NET FW4).

La instalación de .NET FW4 modifica la configuración de IIS ASP.NET registrando el entorno **ASP.NET v4**.

Por ello es muy importante instalar .NET FW4 **despues** de haber completado previamente la instalación de ASP.NET.

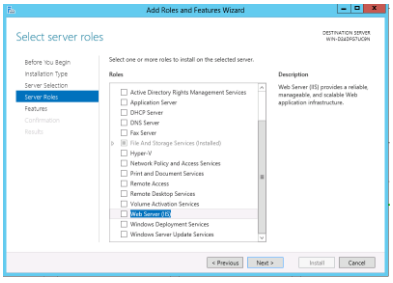
Si instala ASP.NET después de instalar .NET FW4 es posible que el entorno ASP.NET v4 no quede correctamente configurado.

6.3.3 WINDOWS 2012 SERVER

Si va a instalar Evolution en un entorno Windows 2012 Server, le recomendamos que siga los siguientes pasos:

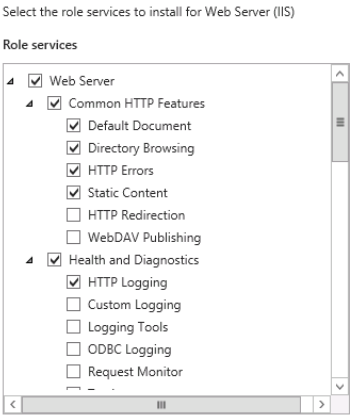
Preparación del entorno Windows 2012 Server

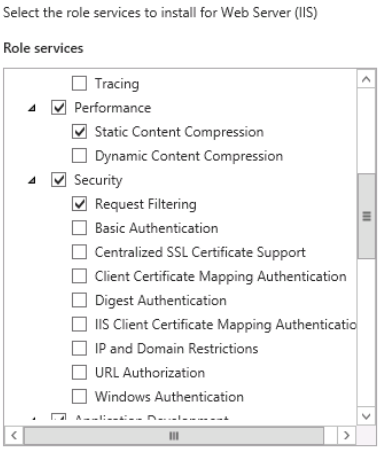
1 *Añada el rol de servidor Web server (IIS)*

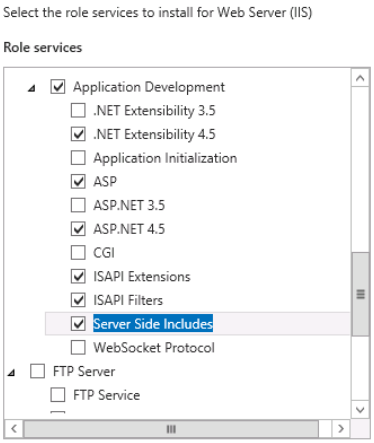


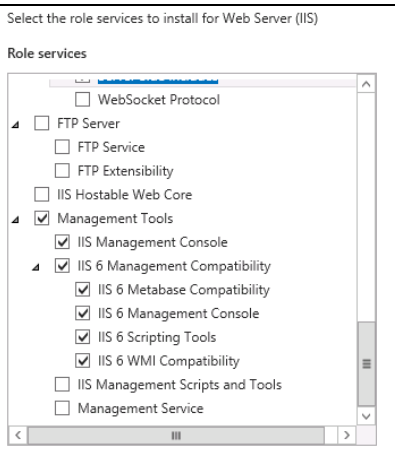
2 Seleccionar las siguientes roles:

- Web Server | Application Development: .NET Extensibility 3.5, .NET Extensibility 4.5
- Añadir ASP, ASP.NET 4.5, ISAPI Extensions, ISAPI Filters, Server Side Includes
- Web Server | Management Tools: IIS Management Consoles y IIS 6 Management Compatibility

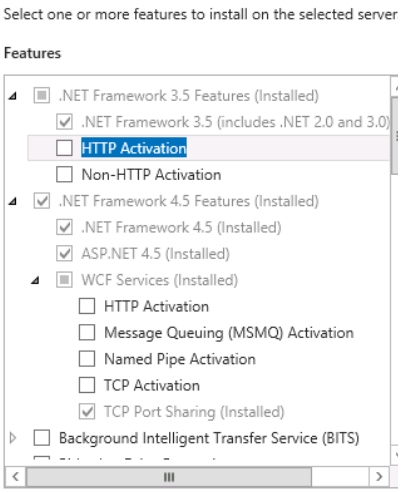








3 Instale la característica “HTTP Activation” para las características (features) de los Frameworks .NET que tenga instalados (.NET Framework 4.5 Features y .NET Framework 3.5 Features)


Select one or more features to install on the selected server
Features
.NET Framework 3.5 Features (Installed)
.NET Framework 3.5 (includes .NET 2.0 and 3.0)
HTTP Activation
Non-HTTP Activation
.NET Framework 4.5 Features (Installed)
.NET Framework 4.5 (Installed)
ASP.NET 4.5 (Installed)
WCF Services (Installed)
HTTP Activation
Message Queuing (MSMQ) Activation
Named Pipe Activation
TCP Activation
TCP Port Sharing (Installed)
Background Intelligent Transfer Service (BITS)

6.4 PREPARACIÓN DEL SERVIDOR SQL SERVER

Evolution almacena sus datos de configuración y campañas en una base de datos Microsoft SQL Server 2005/2008/2012.

Se ha añadido soporte experimental para Microsoft SQL Server 2014.

6.4.1 ACERCA DE MS SQL SERVER 2005

Microsoft ya no ofrece soporte técnico para este producto, y ya no está disponible para su descarga por lo que no vamos a detallar el proceso de instalación paso a paso.

No obstante, Evolution sigue siendo compatible con SQL Server 2005. Le aconsejamos que utilice el último SP del producto (SP4).

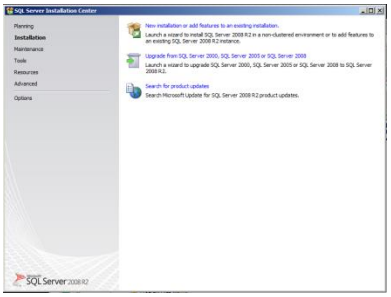
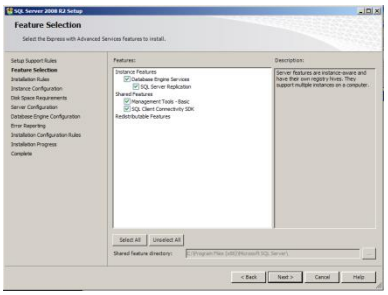
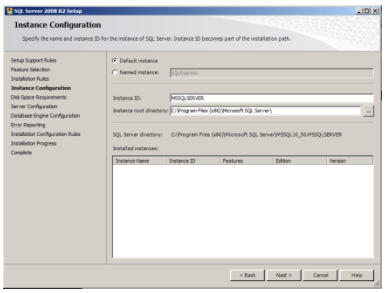
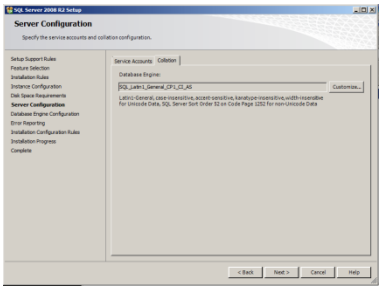
6.4.2 MS SQL SERVER 2008

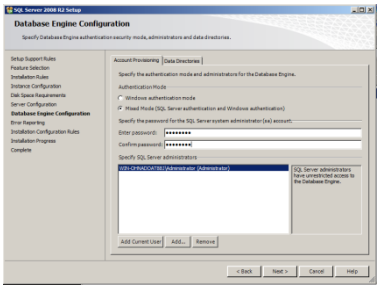
Existe una versión de Microsoft SQL Server 2008 Express Edition gratuita que puede ser útil para entornos de prueba o desarrollo. Usted puede descargar esta versión de la web de Microsoft:
http://www.microsoft.com/express/Database/

Para entornos de producción puede ser recomendable utilizar una edición profesional.

Instalación y configuración del servidor de base de datos MS SQL SERVER 2008

1	Instale y configure el servidor de base de datos MS SQL SERVER 2008 R2 ejecutando el programa de instalación. Si aparece el siguiente aviso *"SQL Server 2008 setup requieres Microsoft.NET Framework and an updated Windows Installer to be installed.* *To enable the .NET Framework Core role, click OK. To exit Setup, click Cancel."* Pulse [OK]

2	Seleccione “New installation or add features to an existing installation” Tras aceptar los términos de licencia de Microsoft se instalaran los diferentes componentes que son requeridos para SQL Server Setup. Resuelva cualquier posible problema que se le muestre antes, de continuar.	
3	En “Feature selection” seleccione “Instance features” (todas) y “shared features” (totas)	
4	En “Instance Configuration” especifique los parámetros más adecuados a sus necesidades particulares. Una configuración válida se consigue marcando “Default instance” y aceptando los valores propuestos por defecto para “Instance ID” (MSSQLSERVER) e “Instance root directory”	
5	En “Server configuration”, pestaña “Collation”, asegúrese que se utiliza un collation order (Intercalado) del tipo CI (Case Insensitive), por ejemplo Modern_Spanish_CI_AS. NOTA: Evolution requiere un collation order (Intercalado) CI (Case Insensitive), por ejemplo Modern_Spanish_CI_AS	

6	En “Database Engine Configuration”, “Account Provisioning”, seleccione la opción Authentication Mode: Mixed Mode (SQL Server authentication and Windows authentication) y especifique un password para la cuenta (sa). En la pestaña “Data Directories” ajuste el “Data root directory”, de acuerdo con sus necesidades. NOTA: Evolution requiere autenticación SQL.	
7	Continúe y complete la instalación de SQL Server 2008 R2	
8	Una vez completada la instalación, ejecute SQL Server Configuration Manager Seleccione “SQL Server Network Configuration”, “Protocols for MSSQLSERVER” y asegúrese que el protocolo TCP/IP está habilitado (status=enabled). Si realiza algún cambio se le indicará que debe reiniciar el servicio SQL Server.	

6.4.3 MS SQL SERVER 2012

Instalación y configuración del servidor de base de datos MS SQL SERVER 2012	
1	Instale y configure el servidor de base de datos MS SQL SERVER 2012 ejecutando el programa de instalación. Si aparece el siguiente aviso *“SQL Server 2008 setup requieres Microsoft.NET Framework and an updated Windows Installer to be installed.* *To enable the .NET Framework Core role,*

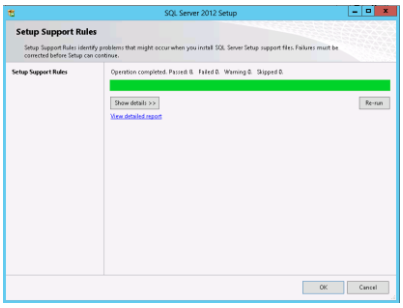
click OK. To exit Setup, click Cancel."

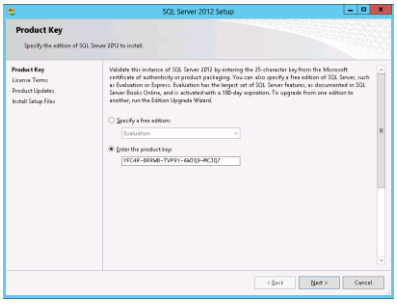
Pulse [OK]

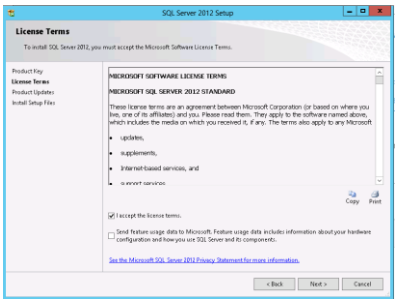
2 Seleccione "New installation or add features to an existing installation"

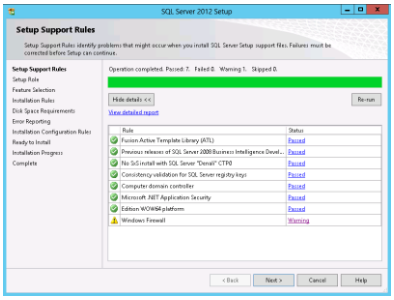
Tras aceptar los términos de licencia de Microsoft se instalaran los diferentes componentes que son requeridos para SQL Server Setup.

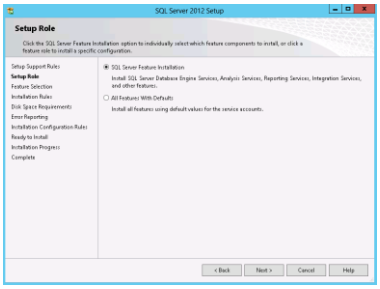
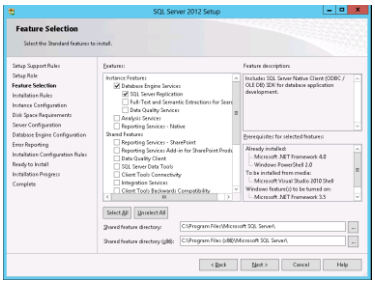
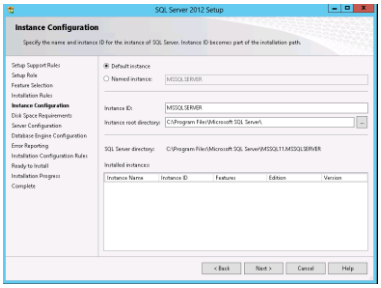
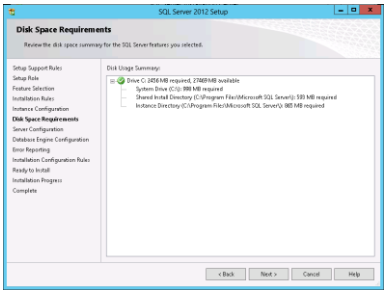
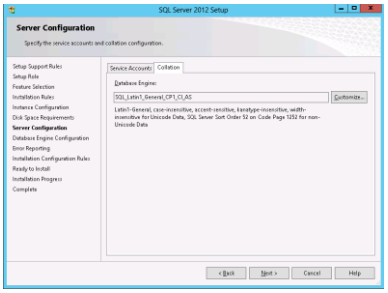
Resuelva cualquier posible problema que se le muestre, antes de continuar.

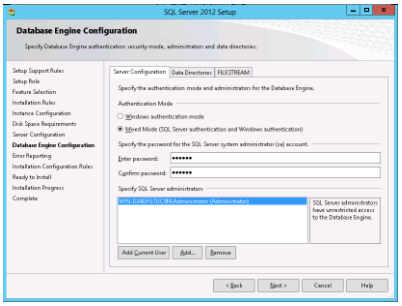
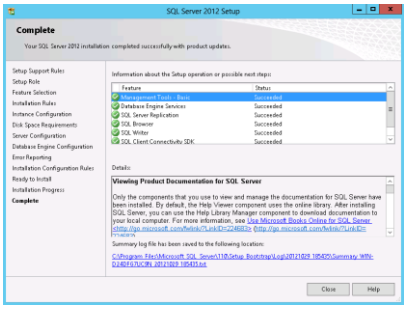








3	En “Setup Role” seleccione “SQL Server Feature Installation”	
4	En “Feature selection” seleccione “Instance features” (todas) y “shared features” (totas)	
5	En “Instance Configuration” especifique los parámetros más adecuados a sus necesidades particulares. Una configuración válida se consigue marcando “Default instance” y aceptando los valores propuestos por defecto para “Instance ID” (MSSQLSERVER) e “Instance root directory”	
6	En “Disk Space Requirements revise el espacio necesario para realizar la instalación	
7	En “Server configuration”, pestaña “Collation”, asegúrese que se utiliza un collation order (Intercalado) del tipo CI (Case Insensitive), por ejemplo SQL_Latin1_General_CP1_CI_AS. NOTA: Evolution requiere un collation order (Intercalado) CI (Case Insensitive), por ejemplo SQL_Latin1_General_CP1_CI_AS	

8	En “Database Engine Configuration”, “Account Provisioning”, seleccione la opción Authentication Mode: Mixed Mode (SQL Server authentication and Windows authentication) y especifique un password para la cuenta (sa). En la pestaña “Data Directories” ajuste el “Data root directory”, de acuerdo con sus necesidades. NOTA: Evolution requiere autenticación SQL.	
9	Continúe y complete la instalación de SQL Server 2012	
10	Una vez completada la instalación, ejecute SQL Server Configuration Manager Seleccione “SQL Server Network Configuration”, “Protocols for MSSQLSERVER” y asegúrese que el protocolo TCP/IP está habilitado (status=enabled). Si realiza algún cambio se le indicará que debe reiniciar el servicio SQL Server.	

6.4.4 CÓMO COMPROBAR EL ORDEN DE INTERCALACIÓN DEL SERVIDOR SQL

Para comprobar el orden de intercalación del servidor (collation order):

1- Ejecute la aplicación de administración de MS SQL Server: SQL Server Management Studio
2- Abrir las "propiedades del servidor": En la raíz del 'treeview' pulsar botón derecho | propiedades
3- Página “General”, parámetro Intercalación del Servidor=Modern_Spanish_CI_AS

6.4.5 CÓMO COMPROBAR EL MODO DE AUTENTICACIÓN DEL SERVIDOR SQL

Para comprobar el modo de autenticación del servidor (server authentication) con SQL Server:

1- Ejecute la aplicación de administración de MS SQL Server: SQL Server Management Studio
2- Abrir las "propiedades del servidor": En la raíz del 'treeview' pulsar botón derecho | propiedades
3- Página “security”, parámetro Server authentication: SQL Server and Windows Authentication mode

6.4.6 CÓMO COMPROBAR EL NOMBRE COMPLETO DE LA INSTANCIA DEL SERVIDOR SQL

Para comprobar el nombre del servidor e instancia con SQL Server:

1- Ejecute la aplicación de administración de MS SQL Server: SQL Server Management Studio
2- Abrir las "propiedades del servidor": En la raíz del 'treeview' pulsar botón derecho | propiedades
3- Seleccione la página “General”, la propiedad “Nombre” indica el nombre completo de la instancia SQL Server. Ejemplo: “SERVER1/SQLSERVEREXPRESS”

6.4.7 CÓMO INSTALAR LAS LIBRERIAS CLIENTE DE MS SQL SERVER

Si prevé instalar la base de datos en un servidor diferente al de Evolution, compruebe que en el servidor de Evolution dispone de los drivers ODBC y conectividad adecuada con el servidor de base de datos.

Obtenga las versiones de drivers ODBC adecuadas a su sistema operativo.

Recuerde que si instala Evoserver sobre SO Windows Server de 64 bits necesitará instalar los drivers SQL tanto de 32 como de 64 bits.

Tenga en cuenta que:

1- Cuando se instala sobre Windows Server (64bits), el servidor Evolution está formado por varios procesos tanto de 32 bits como de 64 bits que requieren conexión con la base de datos de Evolution.
Para ello deberemos instalar los drivers de 32 y 64 bits compatibles con la versión de SQL Server que albergará la base de datos Evolutondb. Por ejemplo, si planeamos utilizar el motor de base de datos Microsoft SQL server 2008 R2, una opción adecuada puede ser instalar el paquete “Microsoft® SQL Server® 2008 R2 Native Client”, X64 Package (sqlncli.msi), contenido en el “Microsoft® SQL Server® 2008 R2 Feature Pack”:
http://www.microsoft.com/en-us/download/details.aspx?id=16978

2- Cuando se instala Evolution sobre Windows Server (64bits) tenga en cuenta que existen dos versiones diferentes de “Administrador ODBC”: C:\windows\system32\odbcad32.exe (64bits) y c:\windows\syswow64\odbcad32.exe (32bits).

3- Evolution Manager permite cargar listas de registros de clientes desde Access, Excel o a partir de ficheros CSV, para lo cual utiliza un origen de datos ODBC denominado “Datos” configurado con el correspondiente driver ODBC. Dado que la versión 64 bits de estos drivers ODBC no se halla preinstalada en Windows 2008

server R2, una opción es instalar el paquete “Microsoft Access Database Engine 2010 Redistributable”: http://www.microsoft.com/downloads/details.aspx?familyid=C06B8369-60DD-4B64-A44B-84B371EDE16D&displaylang=en

6.4.8 RECOMENDACIONES PRÁCTICAS SOBRE LA BASE DE DATOS

El espacio necesario en base de datos varía en función del número de registros de clientes y del número de registros de transacciones que se deseen mantener en las tablas de históricos.

Como primera aproximación, se estima que se requieren unos **5KB** de espacio en la Base de Datos por cada llamada (transacción) a mantener en históricos.

Recomendamos tener en cuenta los siguientes puntos:

1) Siga las mejores prácticas recomendadas por los fabricantes para dimensionar y configurar el hardware del servidor de bases de datos. Tenga en cuenta el impacto positivo sobre el rendimiento que puede obtener si utiliza un sistema de almacenamiento con múltiples unidades de discos.
2) Prevea el crecimiento futuro de la base de datos y reserve con anticipación el espacio necesario en las unidades de disco duro y ficheros de la base de datos. Evite confiar en el modo “autogrowth”.
3) Asegúrese que ha definido “planes de mantenimiento” adecuados en MS SQL Server para mantener optimizados los accesos a los datos mediante índices y tablas. Establezca unos planes periódicos de mantenimiento de los índices y tablas.
4) Mantenga siempre el tamaño de la base de datos en valores adecuados para garantizar que el rendimiento de la solución no se vea afectado negativamente. Tamaños de bases de datos superiores a 10GB no son recomendables.
5) Establezca las políticas de copias de respaldo para evitar la posibilidad de pérdida de datos.
6) Considere la posibilidad de disponer de servidores de alta disponibilidad, como por ejemplo “cluster”.

6.4.9 SOBRE LAS CUENTAS DE USUARIOS DE BASE DE DATOS

La ejecución de la aplicación “setup” de Evolution Server crea automáticamente las bases de datos necesarias en MS SQL SERVER, así como las cuentas de usuario SQL utilizadas para el acceso de los módulos y componentes Evolution a la base de datos :

Estas cuentas son de aplicación y no se corresponden con usuarios concretos del sistema. La modificación de dichas cuentas de usuario podría provocar fallos u errores en el acceso de los diferentes módulos Evolution.

Login NCADMIN
PASSWORD = '”ADMN1cr@”

Login NCAGENTE
PASSWORD = “'AGTE1cr@”

Login NCSUPER
PASSWORD = “SUPR1cr@”

Login NCMAINT
PASSWORD = '”MANT1cr@”

Login SAMSERVER
PASSWORD = “SSRV1cr@”

6.4.10 CÓMO RESTAURAR UNA BASE DE DATOS EVOLUTIONDB

En algunas ocasiones se requiere 'mover' la base de datos EVOLUTIONDB a otro MS SQL server. El proceso recomendado es el siguiente:

1- En el servidor de base de datos de destino deben existir las cuentas de usuario SQL server necesarios para Evolution (NCADMIN, NCAGENTE, NCSUPER, SAMSERVER). La forma más rápida es instalando una base de datos EVOLUTIONDB estándar a través del programa de setup Evolution_server.
2- Restaurar la copia de seguridad de la base de datos EVOLUTIONDB en el nuevo servidor. Para ello se deben seguir los pasos estándar de SQL server para este tipo de operaciones: How to move databases between computers that are running SQL Server

La opción más simple es consiste en hacer esta operación mediante backup/restore, o detach/attach, pero debe tenerse en cuenta que las cuentas de usuario MS SQL no se migran automáticamente, con lo que los usuarios no pueden acceder a la nueva base de datos. Se dice que los usuarios son huérfanos, o “*Orphaned Users*”.

Microsoft documenta varias maneras de resolver este problema de permisos, uno de los cuales se basa en el procedimiento almacenado `sp_change_users_login`

Ver http://support.microsoft.com/kb/314546/en-us

Resumen del procedimiento para reparar ‘orphaned users’:

1- Conectarse a Microsoft SQL Server Management Studio como usuario 'sa', y abrir una nueva consulta SQL.
2- Seleccionar la base de datos EVOLUTIONDB
3- Ejecutar el siguiente procedimiento almacenado:

```
sp_change_users_login 'REPORT'
```

Este procedimiento devuelve una lista de usuarios de la base de datos cuyas credenciales de seguridad no coinciden con las del servidor

4- Para corregir las credenciales de los usuarios NCADMIN, NCAGENTE, NCSUPER, NCMAINT, SAMSERVER, ejecutar los siguientes procedimientos:

```
sp_change_users_login 'AUTO_FIX', 'NCADMIN'

sp_change_users_login 'AUTO_FIX', 'NCAGENTE'

sp_change_users_login 'AUTO_FIX', 'NCSUPER'

sp_change_users_login 'AUTO_FIX', 'NCMAINT'

sp_change_users_login 'AUTO_FIX', 'SAMSERVER'
```

Otros recursos:

- Troubleshoot Orphaned Users (SQL Server) http://technet.microsoft.com/en-us/library/ms175475.aspx
- http://www.mssqltips.com/tip.asp?tip=1590

6.4.11 PROCEDIMIENTOS AUXILIARES PARA MANTENIMIENTO DE ÍNDICES

Los siguientes procedimientos almacenados pueden ser útiles en tareas de mantenimiento.

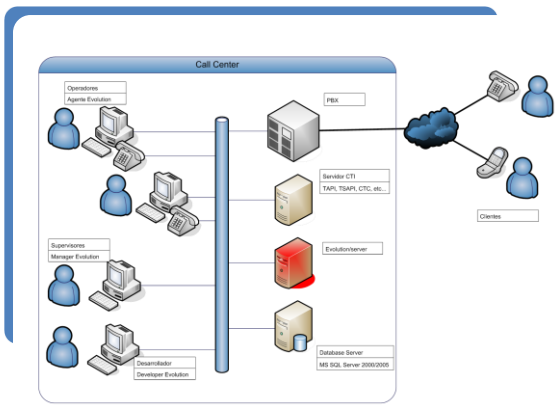
- `sp_DbIndexInfo`: obtiene y muestra información relativa a la fragmentación de índices y tablas de las bases de datos EVOLUTIONDB y EVOLUTIONBDOC.
- `sp_DbOptimize`: reorganiza tablas e índices de las bases de datos EVOLUTIONDB y EVOLUTIONBDOC

6.5 ENLACE CON EL SERVIDOR CTI

Para que el servidor Evolution pueda conectarse a la centralita usted debe instalar un "Servidor CTI" o "Activador CTI" adecuado y configurar correctamente su enlace con la centralita.

Consulte el "16 ANEXO A: Configuraciones de telefonía". Dicho anexo contiene instrucciones paso-a paso para configurar diferentes los tipos de enlace de telefonía.

Switch	Configuración CTI recomendada
AVAYA Aura Communications Manager y AES	AVAYA AURA AES v4 o v5 con TSAPI o CTConnect 7.5 Ver: "16.1 Avaya Aura Communications Manager y AES"
AVAYA IP Office	TAPI, AVAYA IPOffice TAPI3 Service Provider Ver: "16.2 Avaya IP Office"
Avaya CS1000 & CC7	CTConnect 7.5 Ver: "16.3 Avaya CS1000 & CC7"
Nortel Meridian-1 & Symposium 5/6	CTConnect 7.5 Ver: "16.4 Nortel Meridian-1 & Symposium 5/6"
CISCO Communications Manager	TAPI, CISCO TAPI Service Provider Ver "16.5 CISCO Communications Manager CM/UCM"
Panasonic serie TDA/TDE	TAPI, PANASONIC TAPI Service Provider Ver "16.6 Panasonic serie TDA/TDE"
Alcatel Omni PCX Enterprise, ALCATEL 4400	CTConnect 7.5 Ver: "16.7 Alcatel Omni PCX Enterprise, ALCATEL 4400"

Switch	Configuración CTI recomendada
	
IP-PBX Asterisk	TAPI, Activa TSP (TAPI Service Provider) Ver: "16.8 IP-PBX Asterisk"
IP-PBX Asterisk ELASTIX	TAPI, Activa TSP (TAPI Service Provider) Ver: "16.9 IP-PBX Asterisk ELASTIX"
Ericsson MD-110	Application Link 4 con Windows Client CSTA32.DLL
Otras	Consultar a ICR

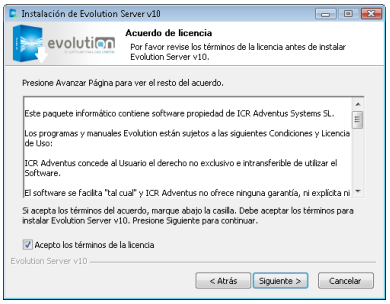
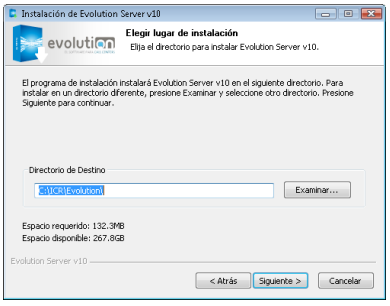
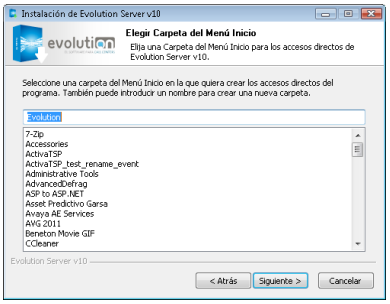
NOTAS Genéricas:

- Los procesos de Evolution server que requieren conectividad con el switch son procesos de 32 bits, así que deberán elegirse librerías adecuadas de 32 bits. En el caso de TAPI se podrán usar drivers TSP de 64 bits.
- Le recomendamos que compruebe la correcta conectividad y funcionamiento del "Servidor CTI" antes de instalar Evolution.

6.6 INSTALACIÓN DEL SERVIDOR EVOLUTION

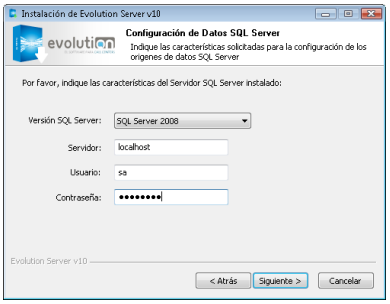
Para instalar el software **Evolution/server** se recomienda seguir el siguiente procedimiento:

Instalación del servidor Evolution/server	
1	*Evolution server requiere .NET Framework 4 (o 4.5 en entorno Windows 2012).* *Si no se encuentra preinstalado en el SO, en este paso del setup se instalará .NET*

	Framework v4 automáticamente. No obstante se recomienda instalarlo con carácter previo	
2	Ejecute la aplicación de instalación del servidor Setup_Evolution_Server_v10.exe	
3	Lea los términos de la **licencia** y acéptelos para continuar la instalación.	
4	Seleccione el **directorio de instalación**. Por defecto se sugiere C:\Program Files\Evolution\.	
5	Seleccione la **carpeta del Menú Inicio**. Por defecto se sugiere Evolution.	

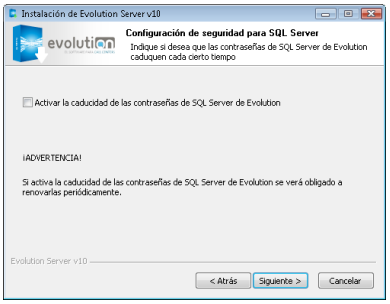
6 Seleccione las características del **Servidor SQL server** instalado:

- Versión SQL Server { SQL Server 2005 SQL Server 2008 o SQL Server 2012}
- Servidor: dirección del servidor SQL
- Usuario/Contraseña[1]: del usuario **sa**

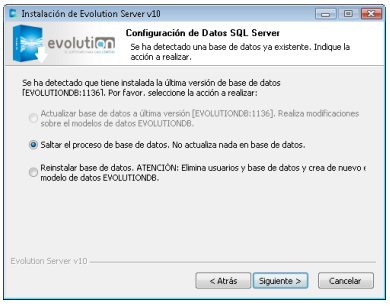


7 Puede activar la caducidad de las contraseñas de las cuentas SQLServer.

*Nota: se recomienda **no activar** la caducidad de las contraseñas SQL. Si se activa la caducidad de de las contraseñas de SQL server de Evolution se verá obligado a renovarlas periódicamente.*


Instalación de Evolution Server v10
Configuración de seguridad para SQL Server
Indique si desea que las contraseñas de SQL Server de Evolution caduquen cada cierto tiempo
Activar la caducidad de las contraseñas de SQL Server de Evolution
¡ADVERTENCIA!
Si activa la caducidad de las contraseñas de SQL Server de Evolution se verá obligado a renovarlas periódicamente.
Evolution Server v10
< Atrás
Siguiente >
Cancelar

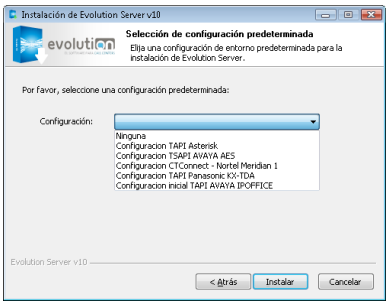
8 Elija una opción o pulse Siguiente para escoger la opción por defecto (recomendada).


Instalación de Evolution Server v10
Configuración de Datos SQL Server
Se ha detectado una base de datos ya existente. Indique la acción a realizar.
Se ha detectado que tiene instalada la última versión de base de datos !EVOLUTIONDB:11361. Por favor, seleccione la acción a realizar:
Actualizar base de datos a última versión [EVOLUTIONDB:1136]. Realiza modificaciones sobre el modelo de datos EVOLUTIONDB.
Saltar el proceso de base de datos. No actualiza nada en base de datos.
Reinstalar base de datos. ATENCIÓN: Elimina usuarios y base de datos y crea de nuevo el modelo de datos EVOLUTIONDB.
Evolution Server v10
< Atrás
Siguiente >
Cancelar

9 El instalador le permite cargar una **configuración predeterminada de parámetros**. Si lo desea, usted podrá reajustar los parámetros posteriormente.

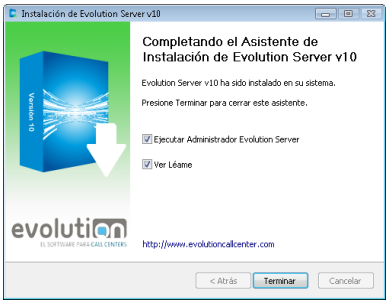
Seleccione una configuración predeterminada de entre las disponibles o seleccione “ninguna” para no modificar una configuración previa existente.

Ej: “Configuración TAPI Asterisk” o “Configuración TSAPI AVAYA”



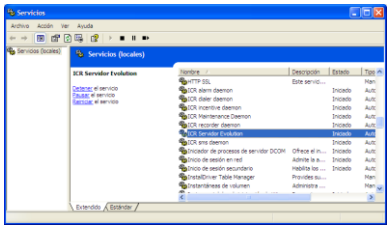
[1] Cuenta de usuario Microsoft SQL Server con permisos suficientes para crear bases de datos.

10 Finalice la instalación y, si es necesario, reinicie el servidor.



11 Compruebe que se han instalado los servicios de Evolution y que están iniciados:

- ICR Dialer Daemon
- ICR Incentive Daemon
- ICR Recorder Daemon
- ICR Servidor Evolution
- ICR Task Daemon
- ICR Router Daemon



12
- Administre el *firewall* de Windows para que los módulos **Evoserver.exe**, **EvoConnector.exe** y **EvoRouterDaemon.exe** puedan recibir conexiones de cliente (red local).

6.7 CONFIGURACIÓN DE LOS PARAMETROS DEL SERVIDOR EVOLUTION

La instalación del servidor establece unos **valores de parámetros por defecto** que son válidos para la mayoría de aplicaciones.

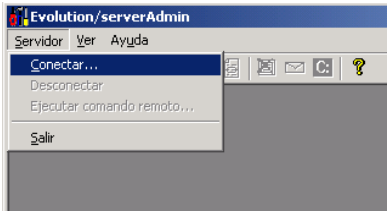
No obstante usted deberá configurar un pequeño número de parámetros ajustándolos a su entorno, en especial los relativos a **tipo de centralita y servidor de telefonía**.

A continuación se describe cómo configurar estos mínimos **parámetros de telefonía** para que Evolution funcione. El resto de parámetros queda documentado en el "Manual de Referencia Evolution".

Configuración de los parámetros del servidor Evolution

1 Ejecute la aplicación de configuración "Administrador Evolution Server" (Evoadmin.exe)...

2 ... y conéctese al servidor. Escriba la direción TCP/IP del equipo donde se ha instalado el servidor.

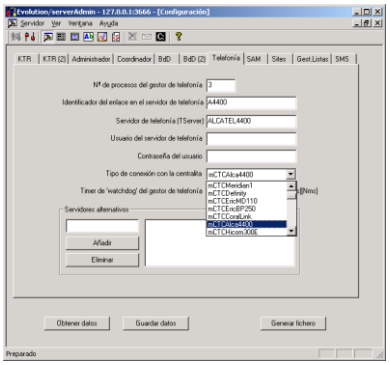


Ej: 192.168.0.100

Si está en el mismo equipo servidor puede utilizar la dirección localhost: 127.0.0.1

El **puerto por defecto** es **3666** y el **password "`admin`". Si no introduce el password el botón "Guardar Datos" quedará deshabilitado**.

3 Si bien el servidor se instala con parámetros por defecto que son válidos en la mayoría de aplicaciones, usted deberá ajustar los **parámetros de telefonía** para adecuarlos a su **tipo de centralita y servidor de telefonía**.



Configure los parámetros de **Configuración | Telefonía** y pulse "Guardar Datos"

NOTA: El significado de estos parámetros está documentado en el apartado **"16 ANEXO A: Configuraciones de telefonía".**

NOTA: La instalación estándar del Servidor Evolution establece la siguiente contraseña para EvoAdmin: "`admin`"

6.8 INTRODUCCIÓN DE LAS LICENCIAS DE EVOLUTION

Si desea licenciar Evolution para activar la edición Enterprise o añadir/eliminar licencias de Evolution para su instalación, utilice la pestaña KTR(2) de la aplicación EvoAdmin.

Las licencias de Evolution dependen de la clave maestra que se genera de forma automática en cada instalación de Evolution. La clave maestra puede consultarse en la pestaña KTR(2) de EvoAdmin.

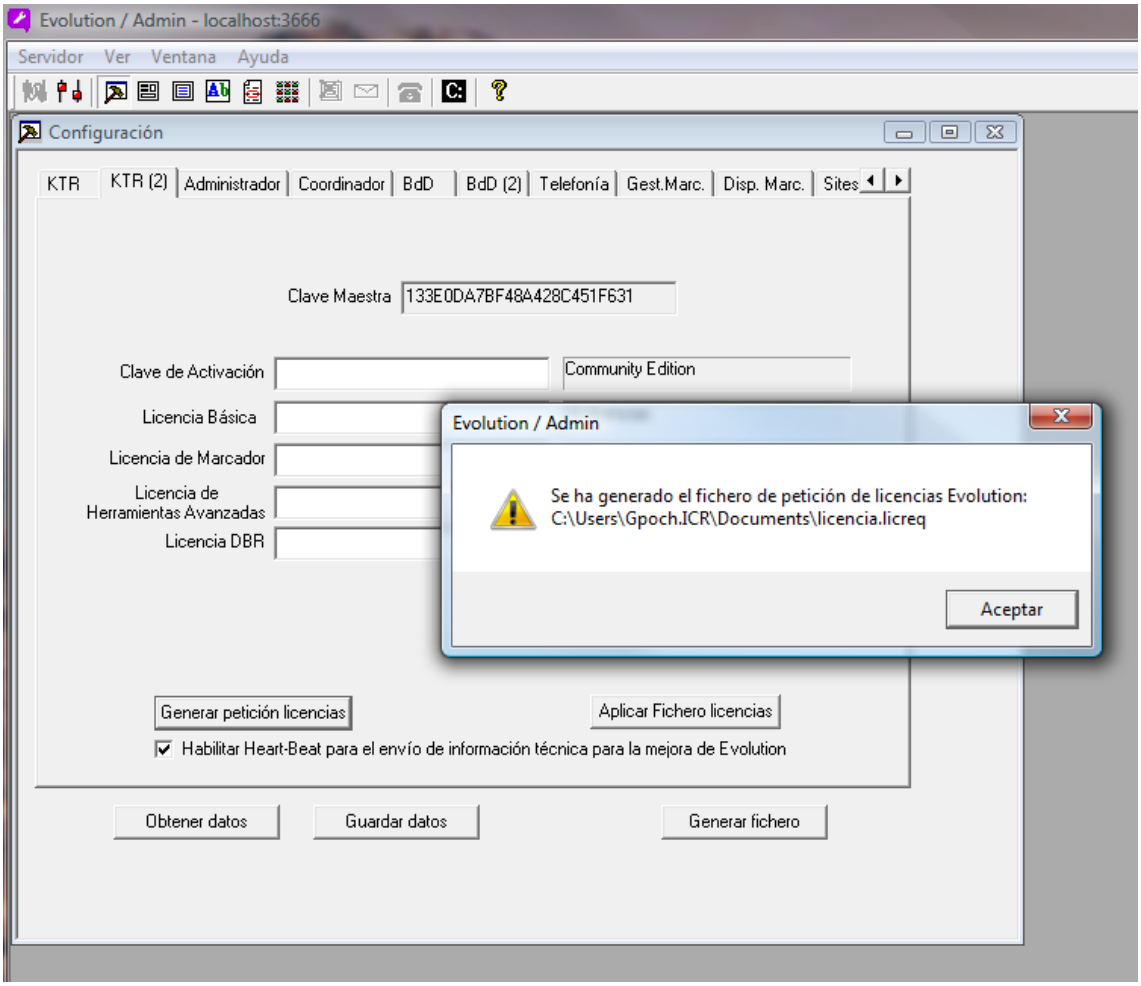
Tenga en cuenta que la clave maestra de Evolution se genera en función del nombre NETBIOS de la máquina y de características propias de la CPU del servidor. Por lo tanto, si usted ejecuta Evolution en un equipo con diferente configuración, las licencias podrían quedar invalidadas.

Recuerde que una vez modificadas las licencias, **debe guardarlas para que tomen efecto**. Para ello, recuerde introducir el password para operaciones restringidas al inicio de EvoAdmin.

6.8.1 PROCESO DE LICENCIA

Este proceso permite enviar una solicitud de licencias y recibir las licencias a través de un fichero.

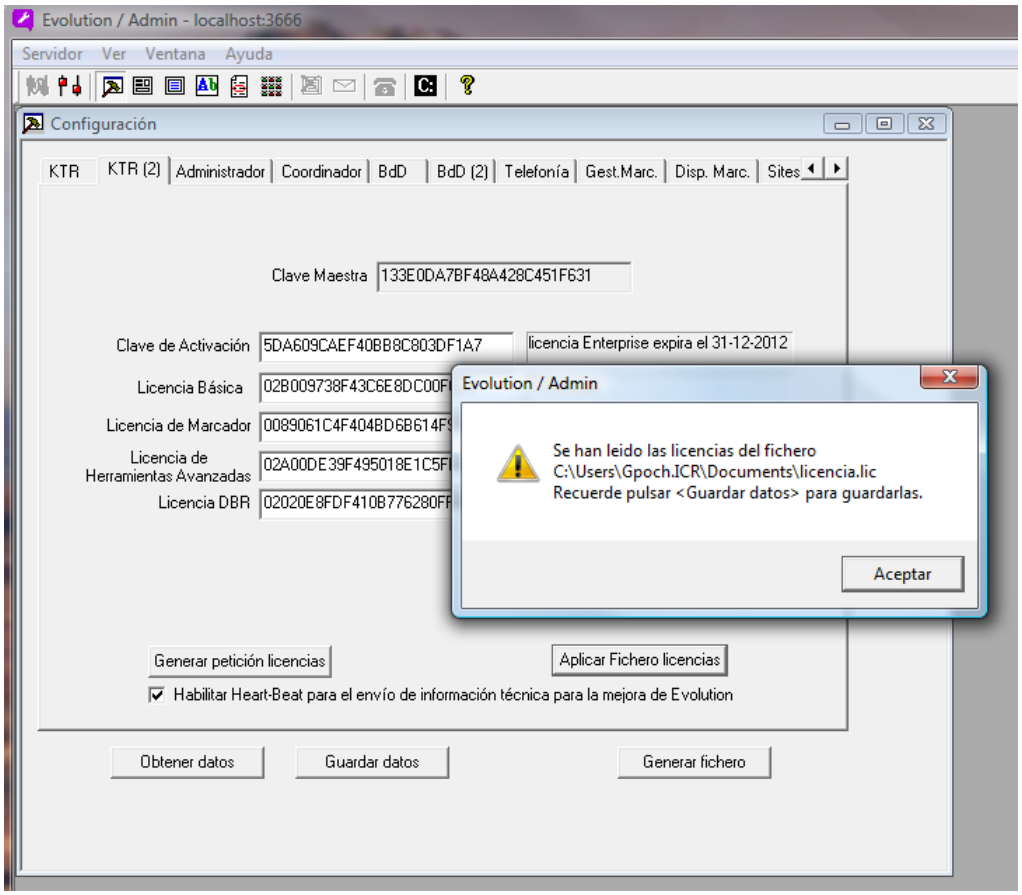
1) Genere el un archivo de petición de licencias pulsando el botón “Generar petición licencias”. Por defecto este archivo se llama licencia.licreq.
    - Se mostrará un diálogo donde podrá especificar el directorio y nombre del fichero donde se guardará la petición de licencias.



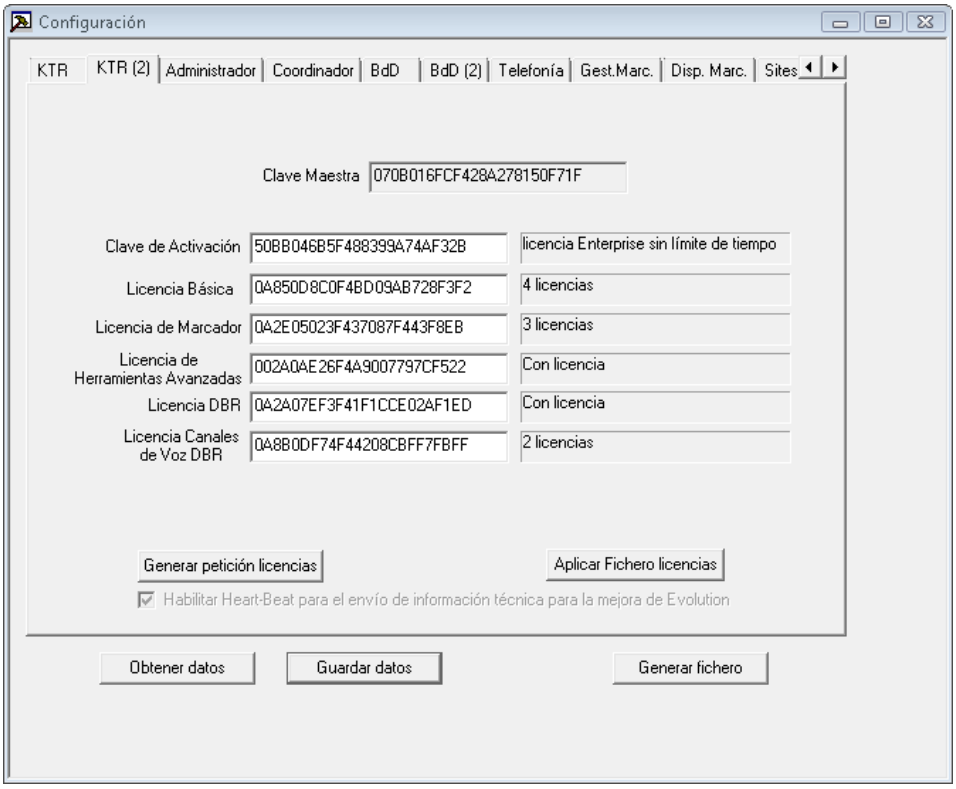
2) Envíe a su proveedor Evolution el archivo generado en el punto 1 junto con los datos identificativos que éste le haya solicitado.

3) Recibirá un archivo con extensión .lic conteniendo las licencias solicitadas. Pulse el botón “Aplicar Fichero licencias” para introducir las claves.

    - Se mostrará un diálogo donde podrá especificar el directorio y nombre donde se encuentra del fichero de de licencias.


Evolution / Admin - localhost:3666
Servidor Ver Ventana Ayuda
Configuración
KTR KTR (2) Administrador Coordinador BdD BdD (2) Telefonía Gest.Marc. Disp. Marc. Sites
Clave Maestra 133E0DA7BF48A428C451F631
Clave de Activación 5DA609CAEF40BB8C803DF1A7
licencia Enterprise expira el 31-12-2012
Licencia Básica
Licencia de Marcador
Licencia de Herramientas Avanzadas
Licencia DBR
Evolution / Admin
Se han leido las licencias del fichero
C:\Users\Gpoch.ICR\Documents\licencia.lic
Recuerde pulsar <Guardar datos> para guardarlas.
Aceptar
Generar petición licencias
Aplicar Fichero licencias
Habilitar Heart-Beat para el envío de información técnica para la mejora de Evolution
Obtener datos
Guardar datos
Generar fichero

4) Pulse el botón “Guardar datos”


Configuración
KTR KTR (2) Administrador Coordinador BdD BdD (2) Telefonía Gest.Marc. Disp. Marc. Sites
Clave Maestra 070B016FCF428A278150F71F
Clave de Activación 50BB046B5F488399A74AF32B
licencia Enterprise sin límite de tiempo
Licencia Básica 0A850D8C0F4BD09AB728F3F2
4 licencias
Licencia de Marcador 0A2E05023F437087F443F8EB
3 licencias
Licencia de Herramientas Avanzadas 002A0AE26F4A9007797CF522
Con licencia
Licencia DBR 0A2A07EF3F41F1CCE02AF1ED
Con licencia
Licencia Canales de Voz DBR 0A8B0DF74F44208CBFF7FBFF
2 licencias
Generar petición licencias
Aplicar Fichero licencias
Habilitar Heart-Beat para el envío de información técnica para la mejora de Evolution
Obtener datos
Guardar datos
Generar fichero

6.9 COMO COMPROBAR EL CORRECTO ACCESO A MANAGER

Manager Evolution es una aplicación web que permite que los supervisores controlen y administren el funcionamiento de las campañas y servicios.

Conexión a Manager

1 Inicie Internet Explorer 8 o superior y navegue a la pagina inicial de Manager:

http://<servername>/manager/

NOTA: La instalación estándar del Servidor Evolution genera un usuario tipo "administrador" con el siguiente login/password: **NCADMIN/NCADMIN.**

6.10 COMO CONFIGURAR LOS PARÁMETROS DE MANAGER

La instalación de Evolution server crea un archivo de configuración `web.config` den el directorio de instalación de Manager (por defecto: C:\inetpub\wwwroot\Manager).

El archivo contiene parámetros estándar que cubren la inmensa mayoría de instalaciones y en general no es necesario modificarlos.

Dependiendo de la arquitectura de telefonía de su call centre puede ser necesario que revise algunos parámetros específicos, como se detalla en el correspondiente el ***"16 ANEXO A: Configuraciones de telefonía".***

Si usted requiere adecuar los parámetros a sus necesidades especficas puede editar dicho archivo:

1- Ubique el archivo de configuración (Por defecto en : `C:\inetpub\wwwroot\Manager\web.config`) y ábralo con un editor de textos (ej: `notepad.exe`)
2- Ubique, en el fichero, la sección `<configuration><appSettings>`
3- Edite los parámetros necesarios y guarde los cambios.

Ejemplo de web.config

NOTA: solo se muestra la sección `appSettings`

```
…/…
        <appSettings>
        <!-- String de conexión a la base de datos evolution-->

        <add key="ConnectionString" value="DSN=EVOLUTIONDB;UID=NCADMIN;PWD=ADMN1cr@;"/>
        <add key="Owner" value="dbo."/>
        <!-- Timeout de la cache de consultas (en segundos) -->
        <add key="TmDbCacheTimeout" value="4"/>
        <!-- Tipo de servidor de base de datos. Actualmente solo se soporta SqlServer = 3-->
        <add key="SQLServer" value="3"/>
        <!-- String de conexión a la base de datos de historicos de evolution-->

        <add key="HistoryConnString" value="DSN=EVOLUTIONDB_HISTO;UID=NCADMIN;PWD=ADMN1cr@;"/>
         <!-- String de conexión al origen de datos para importar clientes-->
         <add key="gConnStrImport" value="DSN=Datos;UID=NCADMIN;PWD=ADMN1cr@"/>
         <!-- Tiempos de refresco-->
         <add key="TmRefreshColas" value="30"/>
         <add key="TmRefreshservicios" value="60"/>
         <add key="TmRefreshAgentes" value="15"/>
         <add key="TmRefreshDatosCampanya" value="60"/>
         <add key="TmRefreshListas" value="60"/>
         <add key="TmRefreshFinales" value="30"/>
         <add key="TmRefreshSegmentos" value="30"/>
         <add key="TmRefreshErrorFrame" value="5"/>
         <!-- Login fail-->
         <add key="MaxLoginTries" value="4"/>
         <add key="TmForgetLoginFail" value="60"/>
         <add key="TmLockUser" value="300"/>
         <!--<add key="Utiles.Traza" value="0"/>-->
         <add key="nFilas" value="10"/>
         <!-- Configuración charts-->
         <add key="ChartImageHandler" value="storage=memory;timeout=1000;"/>
         <!-- Configuración conexión Evoserver-->
         <add key="EvoServer" value="127.0.0.1"/>
         <add key="nMiscPort" value="3777"/>
         <add key="nAdminPort" value="3666"/>
         <add key="TmResponseTimeout" value="5"/>
         <!-- Timeout de informes (segundos), 0 para tiempo infinito-->
         <add key="TmReportTimeout" value="300"/>
         <!-- Timeout de busqueda de clientes (segundos), 0 para tiempo infinito-->
         <add key="TmClientTimeout" value="300"/>
         <!-- Path virtual para almacenamiento de ficheros de Audio -->
         <add key="AudioVirtualDirectory" value="/Manager/Audio/"/>
         <!-- Parametros SFTP para audios de Script DBR -->
         <add key="SFTPHost" value="MyAsterisk"/>
         <add key="SFTPUser" value="root"/>
         <add key="SFTPPort" value="22"/>
         <add key="SFTPPassword" value="MyPassword"/>
         <add key="SFTPRootSounds" value="/var/lib/asterisk/sounds"/>
         <!-- TRAZAS: Path físico para almacenamiento de trazas de Manager.

         Si se deja en blanco equivale a ApplicationPath/Logs -->
         <add key="LogsPath" value=""/>
         <!-- TRAZAS: Número de bytes por fichero -->
         <add key="LogBytes" value="10000000"/>
         <!-- TRAZAS: Número de ficheros -->
         <add key="MaxLogNum" value="10"/>
         <!-- TRAZAS: Escribir a fichero (1/0: SI/NO) -->
         <add key="WriteToFile" value="1"/>
         <!-- path Audio files -->
         <add key="useIdCampanyaAsPath" value="1"/>
         <add key="dateFormatAudioPath" value="yyyy/MM/dd"/>

         <!-- Host AMI -->
         <add key="AMIHost" value="scm" />
```

```
        <!-- Puerto AMI -->
        <add key="AMIPort" value="5038"/>
        <!-- Usuario AMI -->
        <add key="AMIUser" value="evolution"/>
        <!-- Password AMI -->
        <add key="AMISecret" value="bomber"/>

        <!-- WarningLevel: En las páginas de supervisión, umbral de alerta -->
        <add key="WarningLevel" value="80"/>

        <!-- Timeout de la cache de solicitudes de chat (en segundos) -->
        <add key="TmChatRequestTimeout" value="600"/>

        <!-- URL pública del punto de entrada del chat interno agente-supervisor -->
        <add key="WebChatURL"
value="http://evoserver/Evolution/LocalChat/WebChat.aspx?chattype=2&amp;theme=Default&amp;ro
omid={0}&amp;username={1}" />

      </appSettings>
```

6.10.1 CÓMO CONFIGURAR LOS PARÁMETROS DE CHAT INTERNO

Para poder hacer uso de las comunicaciones de chat interno entre agentes y supervisores es necesario configurar en el web.config de Manager la clave "*WebChatURL*". Esta clave viene preconfigurada con la ruta de entrada a la aplicación web LocalChat ya incorporada con Evolution.

En el valor por defecto de esta clave será necesario sustituir "evoserver" por la IP/Nombre del servidor Evolution de manera que la ruta resultante sea accesible tanto desde las aplicaciones de agente como desde la aplicación Manager.

6.11 COMO CONFIGURAR LOS PARÁMETROS DE DEVELOPER-SERVICE

Cuando desde el entorno Developer.NET se genera una aplicación de agentes o DBR-script, ésta se publica por medio de un acceso a un web-service denominado "Developer Service", disponible en el servidor Evolution.

Developer-Service se encarga de la publicación de los diferentes archivos y recursos de las aplicaciones en el servidor y, si es necesario, de sincronizar archivos d eaudio con la plataforma telefónica.

La instalación de Evolution server crea un archivo de configuración `web.config` den el directorio de instalación de Developer-Service (por defecto: C:\inetpub\wwwroot\Evolution\DeveloperService).

El archivo contiene parámetros estándar que cubren la inmensa mayoría de instalaciones y en general no es necesario modificarlos.

Dependiendo de la arquitectura de telefonía de su call centre puede ser necesario que revise algunos parámetros específicos, como se detalla en el correspondiente el ***"16 ANEXO A: Configuraciones de telefonía".***

Si usted requiere adecuar los parámetros a sus necesidades especficas puede editar dicho archivo:

1- Ubique el archivo de configuración (Por defecto en : `C:\inetpub\wwwroot\Evolution\DeveloperService`) y ábralo con un editor de textos (ej: `notepad.exe`)
2- Ubique, en el fichero, la sección `<configuration><appSettings>`
3- Edite los parámetros necesarios y guarde los cambios.

Ejemplo de web.config

NOTA: solo se muestra la sección appSettings

```
<!-- Parametros SFTP para audios de Script DBR -->
<add key="SFTPHost" value="scm" />
<add key="SFTPUser" value="evolution" />
<add key="SFTPPort" value="22" />
<add key="SFTPPassword" value="bomber" />
<!-- Directorio raiz donde se ubicarán las locuciones de los DBRScripts  -->
<add key="SFTPRootSounds" value="/var/lib/asterisk/sounds" />
<!-- Directorio raiz donde se gestiona Music on hold -->
<add key="SFTPRootMoh" value="/etc/asterisk"/>
<!-- Directorio fuente donde se encuentran los Scripts DBR -->
<add key="DBRScripts" value="Evolution/DBRScripts"/>
<!-- Puerto AMI para hacer el reload (el host es igual que el SFTPHost) -->
<add key="AMIPort" value="5038"/>
<!-- Usuario AMI -->
<add key="AMIUser" value="evolution"/>
<!-- Password AMI -->
<add key="AMISecret" value="bomber"/>
```

6.12 CÓMO DESINSTALAR EL SERVIDOR

Para desinstalar el software básico siga el siguiente proceso:

1. Opcionalmente: En caso que usted prevea que posteriormente reinstalará el software, puede ser interesante obtener una copia de seguridad de la base de datos y del registry Windows. Las claves del registry se almacenan bajo `HKLM/software/ICR`.
2. Ejecute en **Panel de Control** ->**Agregar o Quitar Programas**. En la pestaña de **Instalar o Desinstalar** elegir de la lista de software instalado **Evolution Server** y pulsar el botón **Agregar o Quitar** .

Dependiendo de los componentes instalados en su equipo es posible que se mantenga una serie de claves en registry incluso después de desinstalar todos los componentes. Estas claves se encuentran en:

`HKLM/software/ICR`.

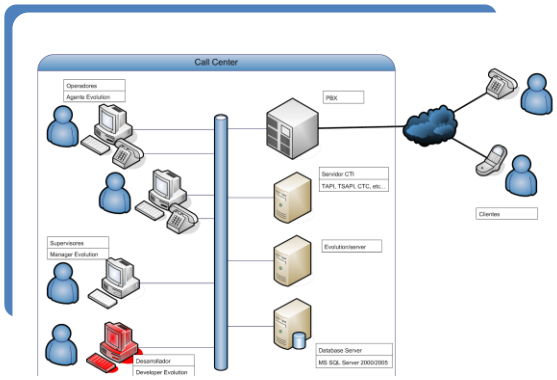
Puede eliminar estas claves manualmente usando `regedit.exe`.

La desinstalación de Evolution Server dejará instalado el jre1.5.0 para evitar posibles conflictos con otras aplicaciones que hagan uso de él. No obstante, se podrá realizar la desinstalación de este componente mediante "Agregar o quitar programas" del "Panel de Control" de Windows.

7 INSTALACION DEL ENTORNO DE DESARROLLO DEVELOPER.NET

Developer.NET permite desarrollar los argumentarios y aplicaciones que se muestran a los teleoperadores cuando gestionan una llamada.

Tambien constituye el entorno de diseño de las aplicaciones DBR-Script, que definen los flujos de llamadas e interacciones en el módulo DBR.



7.1 REQUERIMIENTOS

Requerimientos de software:

Software	Requerimiento
S.O.	Microsoft© Windows XP Microsoft© Windows Vista Microsoft© Windows 7 Microsoft© Windows 8
NAVEGADOR	Microsoft Internet Explorer 8.0 o superior

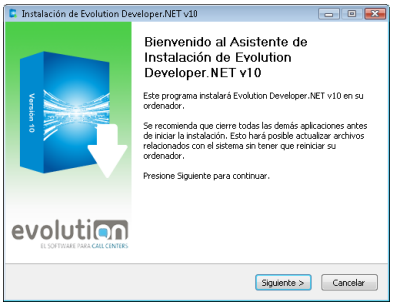
7.2 INSTALACIÓN DE DEVELOPER.NET

Para instalar DEVELOPER.NET EVOLUTION se recomienda seguir el siguiente procedimiento:

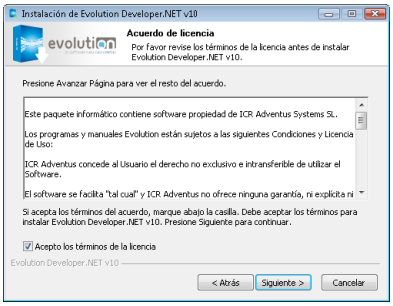
Instalación de DEVELOPER.NET

1 Ejecutar la aplicación de instalación de DEVELOPER.NET EVOLUTION.

Setup_Evolution_Developer.NET_v10.exe

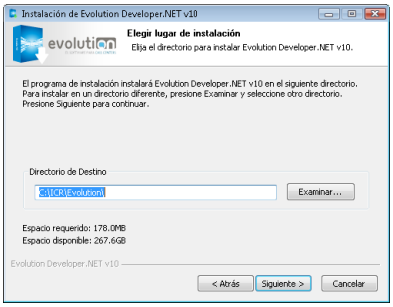

Instalación de Evolution Developer.NET v10
Bienvenido al Asistente de Instalación de Evolution Developer.NET v10
Este programa instalará Evolution Developer.NET v10 en su ordenador.
Se recomienda que cierre todas las demás aplicaciones antes de iniciar la instalación. Esto hará posible actualizar archivos relacionados con el sistema sin tener que reiniciar su ordenador.
Presione Siguiente para continuar.
Versión 10
evolution
Siguiente >
Cancelar

2 Lea los términos de la **licencia** y acéptelos para continuar la instalación.


Instalación de Evolution Developer.NET v10
Acuerdo de licencia
Por favor revise los términos de la licencia antes de instalar Evolution Developer.NET v10.
Presione Avanzar Página para ver el resto del acuerdo.
Este paquete informático contiene software propiedad de ICR Adventus Systems SL.
Los programas y manuales Evolution están sujetos a las siguientes Condiciones y Licencia de Uso:
ICR Adventus concede al Usuario el derecho no exclusivo e intransferible de utilizar el Software.
El software se facilita "tal cual" y ICR Adventus no ofrece ninguna garantía, ni explícita ni
Si acepta los términos del acuerdo, marque abajo la casilla. Debe aceptar los términos para instalar Evolution Developer.NET v10. Presione Siguiente para continuar.
Acepto los términos de la licencia
Evolution Developer.NET v10
< Atrás
Siguiente >
Cancelar

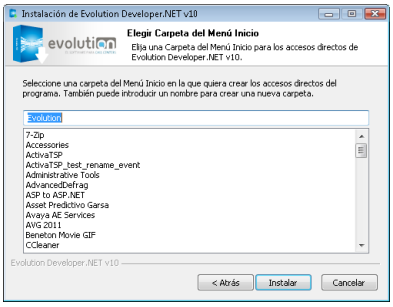
3 Elija el **directorio** de instalación.

Por defecto c:\icr\evolution


Instalación de Evolution Developer.NET v10
Elegir lugar de instalación
Elija el directorio para instalar Evolution Developer.NET v10.
El programa de instalación instalará Evolution Developer.NET v10 en el siguiente directorio. Para instalar en un directorio diferente, presione Examinar y seleccione otro directorio. Presione Siguiente para continuar.
Directorio de Destino
C:\ICR\Evolution\
Examinar...
Espacio requerido: 178.0MB
Espacio disponible: 267.6GB
Evolution Developer.NET v10
< Atrás
Siguiente >
Cancelar

4 Elija la carpeta del menú de inicio.

Por defecto: Evolution



5 Finalice la instalación y ejecute DEVELOPER.NET EVOLUTION

Instalación de Evolution Developer.NET v10
Completando el Asistente de Instalación de Evolution Developer.NET v10
Evolution Developer.NET v10 ha sido instalado en su sistema.
Presione Terminar para cerrar este asistente.
Ejecutar Evolution Developer.NET v10
evolution
< Atrás
Terminar
Cancelar

6 Cuando desde el entorno Developer.NET se genera una aplicación de agentes o DBR-script, ésta se publica por medio de un acceso a un web-service denominado “Developer Service”, disponible en el servidor Evolution.

Developer-Service se encarga de la publicación de los diferentes archivos y recursos de las aplicaciones en el servidor y, si es necesario, de sincronizar archivos d eaudio con la plataforma telefónica.

La instalación de Evolution server crea un archivo de configuración web.config den

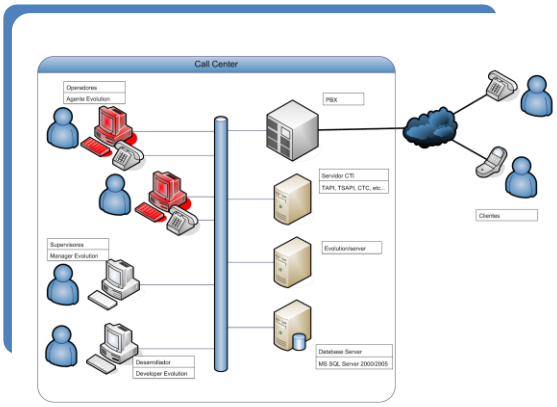
el directorio de instalación de Developer-Service (por defecto: C:\inetpub\wwwroot\Evolution\DeveloperService).

Como configurar los parámetros de Developer-Service

8 INSTALACION DE LA APLICACIÓN IAGENT

La aplicación iAgent Evolution se instala en los PC de los teleoperadores.

Esta aplicación les proporciona el control CTI de las llamadas y les permite acceder a los argumentarios o aplicaciones desarrolladas con developer.NET Evolution y/o otras herramientas.



8.1 REQUERIMIENTOS

Requerimientos de software:

Software	Requerimiento
S.O.	Microsoft© Windows XP Microsoft© Windows Vista Microsoft© Windows 7 Microsoft© Windows 8
NAVEGADOR	Microsoft Internet Explorer 8.0 o superior

Para ejecutar **Evolution iAgent** es necesario que MS Internet Explorer 8.0 esté correctamente instalado y configurado.

8.2 INSTALACIÓN DE LA APLICACIÓN AGENTE

Para instalar la aplicación iAgent se recomienda seguir el siguiente procedimiento:

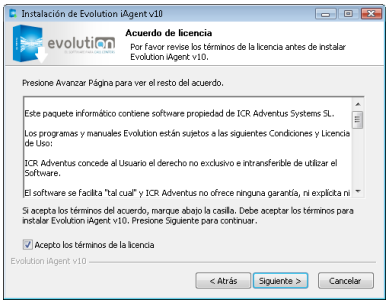
Instalación de iAgent

1 Ejecutar la aplicación de instalación de agente iagent

Setup_Evolution_iAgent_v10.exe

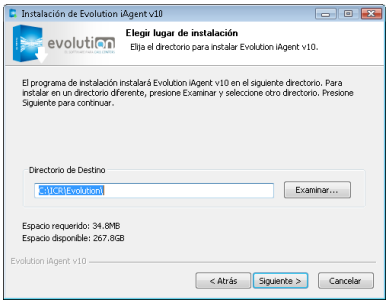
Instalación de Evolution iAgent v10
Bienvenido al Asistente de Instalación de Evolution iAgent v10
Este programa instalará Evolution iAgent v10 en su ordenador.
Se recomienda que cierre todas las demás aplicaciones antes de iniciar la instalación. Esto hará posible actualizar archivos relacionados con el sistema sin tener que reiniciar su ordenador.
Presione Siguiente para continuar.
Versión 10
evolution
Siguiente >
Cancelar

2 Lea los términos de la **licencia** y acéptelos para continuar la instalación.


Instalación de Evolution iAgent v10
Acuerdo de licencia
Por favor revise los términos de la licencia antes de instalar Evolution iAgent v10.
Presione Avanzar Página para ver el resto del acuerdo.
Este paquete informático contiene software propiedad de ICR Adventus Systems SL.
Los programas y manuales Evolution están sujetos a las siguientes Condiciones y Licencia de Uso:
ICR Adventus concede al Usuario el derecho no exclusivo e intransferible de utilizar el Software.
El software se facilita "tal cual" y ICR Adventus no ofrece ninguna garantía, ni explícita ni
Si acepta los términos del acuerdo, marque abajo la casilla. Debe aceptar los términos para instalar Evolution iAgent v10. Presione Siguiente para continuar.
Acepto los términos de la licencia
Evolution iAgent v10
< Atrás
Siguiente >
Cancelar

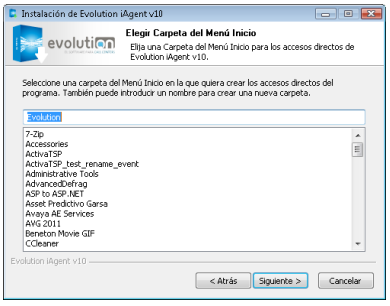
3 Elija el directorio de destino:

Por defecto c:\icr\evolution


Instalación de Evolution iAgent v10
Elegir lugar de instalación
Elija el directorio para instalar Evolution iAgent v10.
El programa de instalación instalará Evolution iAgent v10 en el siguiente directorio. Para instalar en un directorio diferente, presione Examinar y seleccione otro directorio. Presione Siguiente para continuar.
Directorio de Destino
c:\ICR\Evolution\
Examinar...
Espacio requerido: 34.8MB
Espacio disponible: 267.8GB
Evolution iAgent v10
< Atrás
Siguiente >
Cancelar

4 Elija la carpeta del menú de inicio.

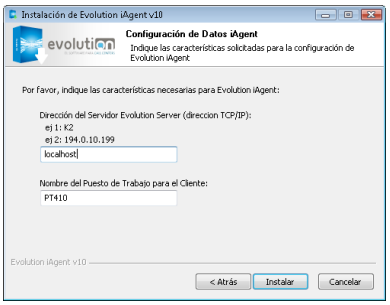
Por defecto: Evolution


Instalación de Evolution iAgent v10
Elegir Carpeta del Menú Inicio
Elija una Carpeta del Menú Inicio para los accesos directos de Evolution iAgent v10.
Seleccione una carpeta del Menú Inicio en la que quiera crear los accesos directos del programa. También puede introducir un nombre para crear una nueva carpeta.
Evolution
7-Zip
Accessories
ActivaTSP
ActivaTSP_test_rename_event
Administrative Tools
AdvancedDefrag
ASP to ASP.NET
Asset Predictivo Garsa
Avaya AE Services
AWG 2011
Beneton Movie GIF
CCleaner
Evolution iAgent v10
< Atrás
Siguiente >
Cancelar

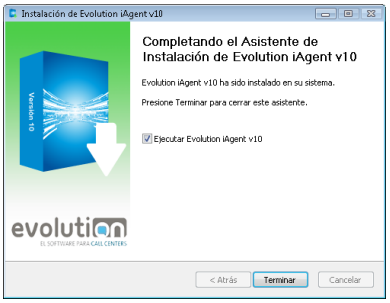
5 Configuración de datos iagent. Especifique los siguientes parámetros:

Dirección del servidor Evolution Server. Ejemplo: server-name

Nombre del Puesto de Trabajo para el Cliente: ejemplo: PT410. Puede dejarlo en blanco si va a usar el softphone integrado en iAgent.


Instalación de Evolution iAgent v10
Configuración de Datos iAgent
Indique las características solicitadas para la configuración de Evolution iAgent
Por favor, indique las características necesarias para Evolution iAgent:
Dirección del Servidor Evolution Server (direccion TCP/IP):
ej 1: K2
ej 2: 194.0.10.199
localhost
Nombre del Puesto de Trabajo para el Cliente:
PT410
Evolution iAgent v10
< Atrás
Instalar
Cancelar

6 Finalice la instalación y ejecute iagent.exe


Instalación de Evolution iAgent v10
Completando el Asistente de Instalación de Evolution iAgent v10
Evolution iAgent v10 ha sido instalado en su sistema.
Presione Terminar para cerrar este asistente.
Ejecutar Evolution iAgent v10
< Atrás
Terminar
Cancelar

NOTA: La instalación estándar del Servidor Evolution genera varios usuarios agente de ejemplo, con los siguientes LOGIN/PASSWORD: AGENTE/AGENTE, AGENTE2/AGENTE2, AGENTE3/AGENTE3, … , AGENTE9/AGENTE9

8.3 PARAMETRIZACIÓN EN REGISTRY

iAgent almacena parámetros en registry Windows 32bits. Los más importantes son los siguientes:

- HKEY_LOCAL_MACHINE\SOFTWARE\ICR\Evolution/iAgent\Global
  - REG_S **Puesto**: Nombre del puesto de trabajo

- HKEY_CURRENT_USER\Software\ICR\Evolution/iAgent\Server
  - REG_SZ: **ServerAddress**: dirección IP para el servidor HTTP de aplicaciones/argumentarios
  - REG_DWORD: Popup: La aplicación se pone en primer plano ante determinados eventos. Default = 1;

- HKEY_CURRENT_USER\ Software\ICR\Evolution/iAgent\Settings
  - REG_DWORD: **DisableContactHistory**: 0=No está deshabilitado el botón de Históricos. Cualquier otro valor numérico=Se deshabilita esta opción. Default value=0.
  - REG_DWORD: **DisableCampaignInfo**: 0=No está deshabilitado el botón de Campañas. Cualquier otro valor numérico=Se deshabilita esta opción. Default value=0.
  - REG_DWORD: **DisablePresencial**: 0=No está deshabilitado el botón de presencial. Cualquier otro valor numérico=Se deshabilita esta opción. Default value=0.
  - REG_DWORD: **ShowScriptErrors**: 0= No se muestran los posibles diálogos de error javascript de la pagina web. Default value=0.

- HKEY_CURRENT_USER\Software\ICR\EvoLink\Settings
  - REG_DWORD **CommTimeout**: timeout comunicaciones, en milisegundos
  - REG_SZ **EvoServerAddress**: dirección IP para el servidor EvoServer
  - REG_DWORD **EvoServerPort**: puerto TCP/IP para conexión al servidor EvoServer.

iAgent incrusta un navegador IE Web Control, para mostrar contenido HTML. El comportamiento de este navegador incrustado puede modificarse mediante parámetros en registry:

- Internet Feature Controls: http://msdn.microsoft.com/en-us/library/ee330720(v=vs.85).aspx

Por defecto, Microsoft IE Web Control funciona en modo emulación IE 7. En algunos casos puede ser recomendable establecer un modo de compatibilidad con una versión IE superior, mediante el parámetro FEATURE_BROWSER_EMULATION:

- HKEY_LOCAL_MACHINE\SOFTWARE\(Wow6432Node)\Microsoft\Internet Explorer\MAIN\FeatureControl\FEATURE_BROWSER_EMULATION

- DWORD:**iagent.exe:** Gobierna el modo de compatibilidad

Por ejemplo: HKEY_LOCAL_MACHINE\SOFTWARE\(Wow6432Node)\Microsoft\Internet Explorer\MAIN\FeatureControl\FEATURE_BROWSER_EMULATION, DWORD:"iagent.exe" = 10001 , habilita el modo de compatibilidad IE 10

Ver "Browser Emulation": http://msdn.microsoft.com/en-us/library/ee330730(v=vs.85).aspx#browser_emulation

8.4 SOPORTE PARA TERMINAL SERVER

El terminal telefónico normalmente está vinculado a un PC concreto y no a un usuario Windows, por lo que la ubicación más adecuada del parámetro "Puesto" es en la rama de **HKEY_LOCAL_MACHINE** del registry Windows.

Pero en determinados casos, como puede ser uso de *softphones* con configuración específica de usuario o el despliegue sobre de Terminal Server, puede requerirse almacenar la información en **HKEY_CURRENT_USER**.

Para ello iAgent lee los parámetros siguiendo el siguiente procedimiento:

1. Si "Puesto" existe en **HKEY_CURRENT_USER**\SOFTWARE\ICR\Evolution/iAgent\Global y NO contiene el valor especial "HKLM", se tomará esta información.
2. En caso contrario, el parámetro "Puesto" se leerá de la ubicación habitual en **HKEY_LOCAL_MACHINE**\SOFTWARE\ICR\Evolution/iAgent\Global

Este esquema permite la configuración en HK_CU, pero al mismo tiempo evitar que, en un entorno terminal server, si UNO de los usuarios instalara en HK_LM, esta situación gobernara a TODOS los usuarios.

9 IAGENTWEBPORTAL: DESPLIEGUE WEB DE LA APLICACIÓN DE AGENTE

La instalación del servidor Evolution despliega un portal web a través del cual los agentes pueden descargar y ejecutar la aplicación de agente.

Por lo general, este tipo de despliegue permite usar la aplicación de agente en entornos en los que el usuario no cuenta con privilegios de administrador o para instalar aplicaciones Windows.

IAGENTWEBPORTAL se basa en la tecnología one-click-deployment, y tiene las siguientes características principales:

- No requiere privilegios de administrador sobre el PC local.
- La aplicación se descarga on-line, y se ejecuta automáticamente.
- Los ficheros se almacenan en una carpeta o caché temporal en el PC del usuario, lo cual reduce o elimina el tiempo necesario para descarga en siguientes sesiones.
- Cada vez que el usuario accede a la aplicación se comprueba automáticamente si dispone de la última versión desplegada en el servidor, y se actualiza si es necesario.

9.1 COMO CONFIGURAR IAGENT WEB PORTAL

La instalación de Evolution server crea un archivo de configuración `web.config` den el directorio de instalación del iagent web portal (por defecto: C:\inetpub\wwwroot\Evolution\ `iAgentWebPortal`).

Si usted requiere adecuar los parámetros a sus necesidades especficas puede editar dicho archivo:

1- Ubique el archivo de configuración (Por defecto en : `C:\inetpub\wwwroot\Evolution\iAgentWebPortal`) y ábralo con un editor de textos (ej: `notepad.exe`)
2- Ubique, en el fichero, la sección `<configuration><appSettings>`
3- Edite los parámetros `EvoServerAddress` y `ScriptServerAddress` e indique valores de dirección IP (hostname o ip-number) que correspondan a puertos accesibles para los agentes.
   a. Ejemplo: `<add key="EvoServerAddress" value="servername"/>`
   b. Ejemplo: `<add key="EvoServerAddress" value="192.168.3.100"/>`
   c. Nota: localhost solo es accesible desde el propio servidor, y por tanto no permite el acceso desde la red de los agentes.
4- Edite los parámetros necesarios y guarde los cambios. Por ejemplo:

Debe tener en cuenta que solo podrán conectarse a través del portal aquellos agentes que dispongan de permisos suficientes. Para asignar permisos a un agente acceda Manager y…

5- Administracion | Usuarios, seleccione el usuario agente al que desea otorgar permisos
6- En el formulario de administración de ese usuario, acceda a “ver roles”
7- Asegúrese de que el agente tiene asignado el rol “Acceso al portal de descarga de la aplicacion agente (click-once)”

NOTA: dicho rol se puede otorgar también a través de grupos de usuarios.

Opcionalmente puede restringir `iAgentWebPortal` para que solamente permita seleccionar puestos de trabajo de un subconjunto. Para ello:

8- Conectese a Manager, y edite una clase de puesto de trabajo
   a. Manager | Administración | Puestos, Ver clases de puesto y edite una clase de puesto. Anote el id correspondiente (.ej: id= 100000003)
   b. Administre los puestos de trabajo deseados y asigneles la clase de puesto anterior
9- Edite web.config y actualice el parámetro `WorktopClassId` con el id deseado
   a. `<add key="WorktopClassId" value="100000003"/>`

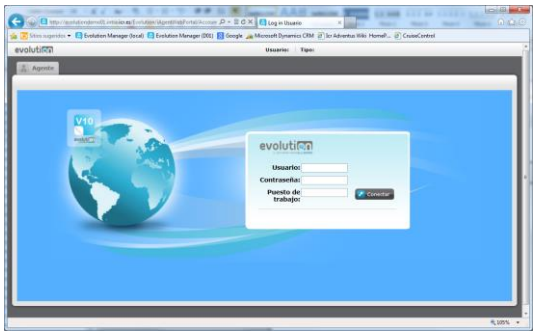
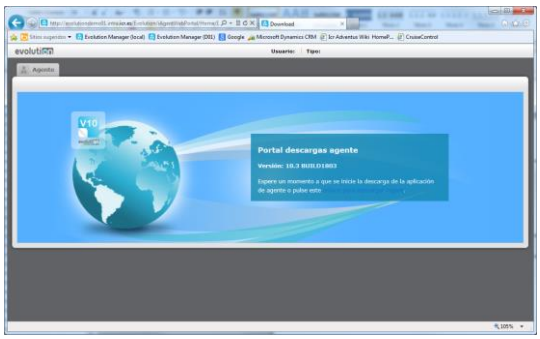
Ejemplo de web.config. NOTA: solo se muestra la sección appSettings

```
    <!-- String de conexión a la base de datos evolution-->
    <add key="ConnectionString" value="DSN=EVOLUTIONDB;UID=NCADMIN;PWD=ADMN1cr@;"/>
    <add key="Owner" value="dbo."/>

    <!-- EvoServerAddress debe configurarse con la ip del servidor evoserver.exe -->
    <add key="EvoServerAddress" value="localhost"/>
    <!-- EvoServerPort debe configurarse con el puerto ip del servidor evoserver.exe,
 ej: 3555, o 35555 -->
    <add key="EvoServerPort" value="3555"/>
    <!-- ScriptServerAddress debe configurarse con la ip del servidor de scripts -->
    <add key="ScriptServerAddress" value="localhost"/>
    <!--
 opcional: puede indicarse un idclasepuestotrabajo para restringir los PT admitidos.
Ej: IdClasePuestoTrabajo=100000004 -->
    <add key="WorktopClassId" value="0"/>

    <!-- TRAZAS: Path físico para almacenamiento de trazas de Manager.

         Si se deja en blanco equivale a ApplicationPath/Logs -->
    <add key="LogsPath" value=""/>
    <!-- TRAZAS: Número de bytes por fichero -->
    <add key="LogBytes" value="10000000"/>
    <!-- TRAZAS: Número de ficheros -->
    <add key="MaxLogNum" value="10"/>
    <!-- TRAZAS: Escribir a fichero (1/0: SI/NO) -->
    <add key="WriteToFile" value="1"/>
    <add key="Debug" value="false"/>
```

9.2 COMO SE ACCEDE A IAGENT WEB PORTAL

Para acceder a la aplicación agente desde iAgentWebPortal

Acceso a la aplicación agente desde iAgentWebPortal

1	Ejecute el navegador Internet Explorer (versión 9 o superior) y navege al portal iAgentWebPortal: http://<evolutionserver>/Evolution/iAgentWebPortal/ …donde <evolutionserver>debe ser la dirección del servidor Evolution	
2	Informe los siguientes parámetros: Usuario: login del agente Evolution Contraseña: contraseña del usuario Puesto Trabajo: Puesto de trabajo al que desea conectarse. Como ayuda se le mostrará una lista de coincidencias (*autocomplete*)	
3	Al pulsar Conectar el servidor tratará de autenticar su nombre de usuario y contraseña proporcionados. Si la validación es correcta s se mostrará una página de descarga, que s einiciará automáticamente. NOTA: La descarga esta sujeta a que el usuario Evolution disponge de privilegios adecuados en Manager. Pueden acceder al portal de agente aquellos agentes que tengan asignado el ROL de permisos “desde portal de agentes”	
4	Si la descarga no se iniciara automáticamente puede pulsar el enlace que se proporciona en la propia página.	

5 Una ventana le informará del progreso de la descarga, y le pedirá que acepte el certificado de la misma.

Finalmente la aplicación de agente se iniciará, automáticamente.

10 INSTALACIÓN DEL SERVIDOR WEBCHAT

El servidor WebChat es el módulo de Evolution que aloja la aplicación web que permite la integración de un chat con Evolution haciendo uso del conector DBR WebServiceAPI.

Este módulo contiene la lógica que permite a los clientes contactar vía Chat y ser atendidos por un agente Evolution a través del mismo medio.

10.1 REQUERIMIENTOS

Para instalar y ejecutar **Evolution WebChat** se requiere el siguiente software:

Software	Requerimiento
S.O.	Microsoft© Windows 2003 R2 Microsoft© Windows 2008 (32 bits) Microsoft© Windows 2008 R2 (64 bits) Microsoft© Windows 2012 (64 bits) Microsoft© Windows 2012 R2 (64 bits)
Servidor WEB	MS IIS con ASP.NET v4 instalado

Versión certificada: Microsoft© Windows 2008 R2 (64 bits) con IIS 7.5

10.2 INSTALACIÓN

Para instalar EVOLUTION WEBCHAT se recomienda seguir el siguiente procedimiento:

Instalación de Evolution WebChat

1 *Evolution WebChat requiere .NET Framework 4.*

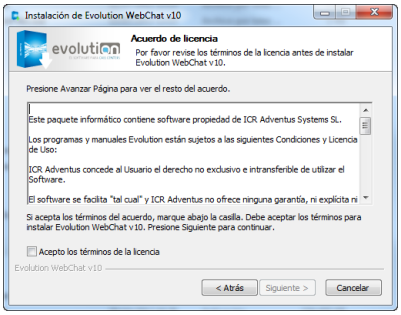
Si no se encuentra preinstalado en el SO, en este paso del setup se instalará .NET Framework v4 automáticamente. No obstante se recomienda pre-instalarlo con carácter previo

2 Ejecutar la aplicación de instalación de EVOLUTION WEBCHAT.

Setup_Evolution_WebChat_v10.exe

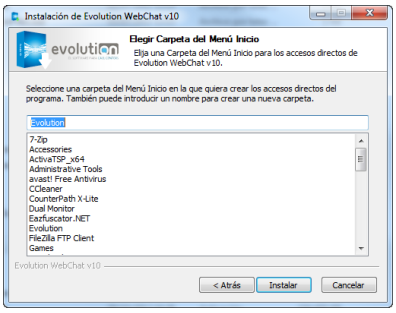
Instalación de Evolution WebChat v10
Bienvenido al Asistente de Instalación de Evolution WebChat v10
Este programa instalará Evolution WebChat v 10 en su ordenador.
Se recomienda que cierre todas las demás aplicaciones antes de iniciar la instalación. Esto hará posible actualizar archivos relacionados con el sistema sin tener que reiniciar su ordenador.
Presione Siguiente para continuar.
Siguiente >
Cancelar

3 Lea los términos de la **licencia** y acéptelos para continuar la instalación.

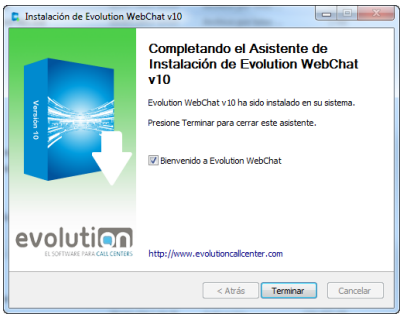

Instalación de Evolution WebChat v10
Acuerdo de licencia
Por favor revise los términos de la licencia antes de instalar Evolution WebChat v10.
Presione Avanzar Página para ver el resto del acuerdo.
Este paquete informático contiene software propiedad de ICR Adventus Systems SL.
Los programas y manuales Evolution están sujetos a las siguientes Condiciones y Licencia de Uso:
ICR Adventus concede al Usuario el derecho no exclusivo e intransferible de utilizar el Software.
El software se facilita "tal cual" y ICR Adventus no ofrece ninguna garantía, ni explícita ni
Si acepta los términos del acuerdo, marque abajo la casilla. Debe aceptar los términos para instalar Evolution WebChat v10. Presione Siguiente para continuar.
Acepto los términos de la licencia
Evolution WebChat v10
< Atrás
Siguiente >
Cancelar

4 Elija la carpeta del menú de inicio.

Por defecto: Evolution



5 Finalice la instalación.


Instalación de Evolution WebChat v10
Completando el Asistente de Instalación de Evolution WebChat v10
Evolution WebChat v10 ha sido instalado en su sistema.
Presione Terminar para cerrar este asistente.
Bienvenido a Evolution WebChat
http://www.evolutioncallcenter.com
< Atrás
Terminar
Cancelar

10.3 CONFIGURACIÓN DE LOS PARAMETROS DE WEBCHAT

La instalación del servidor establece unos **valores de parámetros por defecto** que son válidos para la mayoría de instalaciones.

No obstante usted deberá configurar un pequeño número de parámetros ajustándolos a su entorno, en especial los relativos a la conectividad con el **servidor Evolution.**

10.3.1 CONFIGURACIÓN DE WEB.CONFIG

El archivo *web.config* de la aplicación se encuentra en el directorio de instalación de WebChat (por defecto: `C:\inetpub\wwwroot\Evolution\WebChat`).

En la sección `<appSettings>` la clave **`EvoRouterAPIAddress`** deberá actualizarse con el valor adecuado para que apunte al conector DBR WebServiceAPI (por ejemplo `http://EvolutionServer:3664/EvoRouterAPI`).

También sera necesario configurar el parámetro *address* de la clave <endpoint>que se encuentra bajo <system.serviceModel> <client> <endpoint **address**="http://localhost:3664/EvoRouterAPI"> indicando la dirección del conector DBR WebServiceAPI del servidor Evolution.

10.3.2 CONFIGURACIÓN POR TEMAS

Por otra parte, Evolution WebChat permite la personalización del aspecto del chat y de parte de su comportamiento a través del uso de temas ASP.NET. Esto permite disponer de diferentes temas para dar una respuesta personalizada para diferentes clientes o situaciones.

A modo de ejemplo, Evolution WebChat, instala dos temas: Default y Blue (por defecto se encuentran bajo `C:\inetpub\wwwroot\Evolution\WebChat\App_Themes`). Cada tema incluye los graficos, las hojas de estilo y el resto de recursos necesarios para la personalización del chat.

Entre estos recursos se encuentra el archivo *appSettings.config* que permite configurar algunos aspectos de comportamiento, como la verificación de integridad de la URL mediante hash y su contraseña o algunos de los textos de sistema que se muestran en el chat.

Claves de control:

```
<add key="ThemeName" value="Default" />
<add key="UserTimeout" value="20" /> <!-- Timeout de usuarios en segundos -->
<add key="ErrorPage" value="WebChatError.aspx" />
<add key="HashSecured" value="true" />
<add key="HashSecret"  value="abcde" />
```

Claves de textos:

```
<add key="Send" value="Enviar" />
<add key="SendFile" value="Enviar fichero" />
<add key="Upload" value="Subir" />
<add key="ChatDisconnected" value="Chat finalizado" />
<add key="ChatRoomName" value="WebChat" />
<add key="NewUser" value="El usuario {0} ha entrado en el chat." />
<add key="ChatRoomTopic" value="Bienvenido a Evolution WebChat!" />
<add key="UsersOnline" value="Usuarios conectados" />
<add key="QueuedMessage" value="Su petición de chat está en cola de espera y será atendida por un agente tan pronto como sea posible." />
<add key="QueuePosition" value="Su posición en cola es: {0}" />
<add key="QueueExpectedWaitTime" value="Su tiempo estimado de espera es de {0} segundos." />
<add key="MsgUserHasLeft" value="El usuario {0} ha abandonado el chat." />
<add key="ErrorMessage" value="Lo sentimos, pero en estos momentos no podemos atender su solicitud. Por favor, inténtelo de nuevo más tarde." />
```

10.4 CÓMO INICIAR UNA SESIÓN CON WEBCHAT

Evolution WebChat dispone de un punto de entrada único (*WebChat.aspx*). Esta página web encola automáticamente la petición en el servidor Evolution y crea una nueva sesión de chat en la que el cliente permanecerá a la espera de ser atendido por un agente.

La petición de chat se cursa a través de una cola DBR del call center de forma que, cuando un agente quede libre, recibirá la petición de web-chat, y podrá conectarse con el cliente a través de la sesión chat ya iniciada.

Para implementar el acceso de usuarios al chat desde una aplicación cliente será necesario enlazar con la página WebChat.aspx pasando como parámetros:

Parámetros	
theme	Tema ASP.NET para la visualización del chat. Ejemplo: Default
username	Nombre que identifica al cliente. Ejemplo: Pepe
strategy	Estrategia de enrutamiento Evolution. Ejemplo: Chat1
hash (opcional según configuración)	En caso de estar activada la verificación de integridad de la URL en el tema, el hash MD5 de los parámetros de la URL + Secret Key (opcional). Ejemplo: 2285c84cf672e61730391118f4cdb2f6

Opcionalmente, también es posible pasar parámetros arbitrarios adicionales (ej: teléfono, nombre, etc) a la página de inicio de chat. Estos parámetros se trasladarán como propiedades del documento DBR encolado.

En la carpeta de instalación (típicamente, *C:\Archivos de programa\Evolution\WebChat*) encontrará un ejemplo básico de aplicación cliente que inicia una sesión de chat (*NewChatSample.htm*).

10.5 INSTALACIÓN DE VIDEOCHAT

Para poder disponer de la opción de VideoChat será necesaria la instalación de Flash Media Server o RED5 en el servidor de chat.

Flash Media Server es el servidor multimedia de Adobe que permite la comunicación de datos, audio y video en tiempo real. Red5 es un 'clon' de Flash Media Server que es open-source y gratuito.

En este manual daremos unas instrucciones básicas para configurar el VideoChat con Red5.

10.5.1 INSTALACIÓN DEL SERVIDOR RED5

Para instalar el servidor Red5 hay que seguir los siguientes pasos:

- **Descargar el instalador**. Se puede descargar desde http://www.red5.org/downloads/red5/. Seleccionar el instalador adecuado para el sistema operativo.

- **Instalación de JRE**. Se puede descargar la última versión desde http://www.java.com/es/download/windows_xpi.jsp. Recuerde descargar la versión correcta para el sistema operativo Windows dependiendo de si este es de 32 o 64 bits.

- **Instalación del servidor RED5:** Ejecute el instalador de Red5. Por defecto se instala en **C:\Program Files\Red5** o en **C:\Program Files (x86)\Red5** para sistemas de 64 bits. Cuando pregunte por una dirección IP hay que introducir una IP estática para que desde otros equipos se pueda acceder al servidor red5 (*Red5IPServer*). Cuando pregunte por un puerto hay que introducir **5080**.

- **Comprobar el servicio RED5:** En la lista de Servicios buscamos el servicio RED5 y comprobamos que está habilitado e iniciado.

- **Comprobar el servidor RED5:** Para probar si se instaló RED5 abrimos el siguiente URL en un navegador **http://*Red5IPServer*:5080/**. La página de RED5 debe aparecer y, si lo hace, la instalación se realizó satisfactoriamente.

Puede encontrar más información al respecto del servidor Red5 en http://www.red5.org.

10.5.2 CONFIGURACIÓN DE VIDEOCHAT

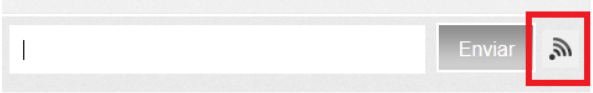
Para configurar el VideoChat sólo será necesario indicar la IP del servidor Red5 en el archivo Web.config de WebChat.

En la sección `<applicationSettings>` `<eStreamChat.Properties.Settings>` será necesario configurar el setting "FlashMediaServer" indicando la dirección del servidor Red5.

```
<applicationSettings>
    <eStreamChat.Properties.Settings>

      <setting name="FlashMediaServer" serializeAs="String">
        <value>rtmp://Red5IPServer/live</value>
      </setting>

    </eStreamChat.Properties.Settings>
  </applicationSettings>
```

10.5.3 VERIFICACIÓN DE VIDEOCHAT

Para probar si el VideoChat está correctamente instalado y configurado, podemos comprobar que, si se establece una sesión de chat desde una máquina con cámara activada, aparece un icono en la parte inferior del chat.



Si pulsamos sobre el icono, WebChat pedirá permiso para acceder a cámara y micrófono.

Broadcast Video
Configuración de Adobe Flash Player
Acceso a cámara y micrófono
localhost solicita el acceso a su cámara y micrófono. Si hace clic en Permitir, podrá ser grabado.
Permitir
Denegar

Una vez permitido el acceso, debe aparecer la imagen de video en pantalla. Si lo hace, la instalación/configuración se realizó satisfactoriamente.

10.6 SECURIZACIÓN DE LAS COMUNICACIONES WEBCHAT

Existen dos posibles niveles de securización de las comunicaciones de Evolution WebChat:

- URL con hash de encriptación MD5
- Encriptación SSL

10.6.1 VERIFICACIÓN DE INTEGRIDAD DE LA URL

Modificando el archivo *appSettings.config* contenido en cada tema ASP.NET del servidor WebChat es posible activar/desactivar la verificación de integridad de la URL e indicar la clave privada para la encriptación (Claves <HashSecured> y <HashSecret>).

El objectivo de usar una clave privada adicional es el de añadir mayor seguridad haciendo uso de un Salted Hash que consiste en simplemente añadir una cadena secreta de caracteres (HashSecret) a los parámetros de la URL antes de calcular su hash.

Por tanto, si la verificación hash está activada, en la llamada URL al punto de entrada de WebChat (*WebChat.aspx*) deberá indicarse un parámetro adicional (hash) que estará formado a partir de una funcion de hash (md5) donde el parámetro es la concatenación de la cadena de parámetros URL + HashSecret.

Por ejemplo, si la llamada es http://localhost/Evolution/WebChat/WebChat.aspx?theme=Default&username=Pepe&strategy=Chat1 y la clave secreta es '*abcde*'el valor de hash sería el resultado de calcular el valor encriptado MD5 de "*theme=Default&username=Pepe&strategy=Chat1*" + "*abcde*".

Así pues, la llamada URL al punto de entrada de WebChat tendría la siguiente forma:

> http://localhost/Evolution/WebChat/WebChat.aspx?theme=Default&username=Pepe&strategy=Chat1&hash=2285c84cf672e61730391118f4cdb2f6

10.6.2 PUBLICACIÓN HTTPS

Para poder publicar Evolution WebChat en HTTPS sólo será necesario seguir las indicaciones de Securización de las comunicaciones de este mismo documento.

11 TASK DAEMON

Este módulo es el responsable de realizar algunas tareas importantes de base de datos: traspaso diario de información a tablas de datos históricos, carga de los registros en las listas de las campañas, borrado y limpieza de campañas y usuarios, etc. Pero también se encarga de dar soporte a EvoServer en algunos cálculos relacionados con segmentos dinámicos.

11.1 COMO MODIFICAR LA CONFIGURACIÓN DEL SERVICIO TASK DAEMON

Se puede modificar su configuración por defecto a través de dos claves del registro de sistema, los parámetros principales son los siguientes:

11.1.1 COMUNICACIÓN CON EVOSERVER Y CONFIGURACIÓN DEL SERVICIO

En la clave: **HKEY_LOCAL_MACHINE\SOFTWARE\ICR\EvoTaskDaemon**

- REG_SZ **DbConnectionString**: cadena de conexión con a la base de datos (por defecto "DSN=EVOLUTIONDB;UID=NCADMIN;PWD=ADMN1cr@;").
- REG_SZ **LogFile**: archivo de trazas (por defecto EvoTaskDaemon.log)
- REG_DWORD **MaxLogNum**: máximo número de archivos de trazas (rotativo) (por defecto 10).
- REG_DWORD **LogBytes**: tamaño máximo de los archivos de trazas (por defecto 10000000)
- REG_DWORD **LogLevel**: nivel de detalle de las trazas, los valores válidos van desde 0: máximo detalle, hasta 5: sin trazas (por defecto 1).
- REG_DWORD **WriteLogToFile**: indica si se han de guardar las trazas en fichero si(1) o no(0) (por defecto 1).

11.1.2 MANTENIMIENTO DE LA BASE DE DATOS

En la clave: **HKEY_LOCAL_MACHINE\SOFTWARE\ICR\MaintenanceDaemon**

- REG_SZ **DbCommandTimeout**: tiempo máximo (en segundos) que tienen los comandos de SQL para ejecutarse (por defecto 30).
- REG_SZ **DbConnectionString**:cadena de conexión con a la base de datos (por defecto "DSN=EVOLUTIONDB;UID=NCADMIN;PWD=ADMN1cr@;").
- REG_SZ **DbDocConnectionString**: cadena de conexión a la base de datos de documentos (por defecto "DSN=EVOLUTIONDBDOC;UID=NCADMIN;PWD=ADMN1cr@;").
- REG_SZ **DbHistoConnectionString**: cadena de conexión a la base de datos de históricos (por defecto "DSN=EVOLUTIONDB_HISTO;UID=NCADMIN;PWD=ADMN1cr@;").
- REG_SZ **DbMaintConnectionString**: cadena de conexión a la base de datos de históricos (por defecto "DSN=EVOLUTIONDB;UID=NCMAINT;PWD=MANT1cr@;").
- REG_DWORD **DbMaxRows**: tamaño de los bloques de datos para las operaciones (por defecto 1000).
- REG_DWORD **DbOptimzeTimeout**: tiempo máximo (en segundos) que tienen los comandos de optimización de la base de datos para ejecutarse (por defecto 7200).

- REG_DWORD **DiasHistoricoCubo**: número de días que se conservará la información en las tablas de históricos (por defecto -1).
    - -1: indicado en la configuración de la campaña. *Dado que el registro de Windows no admite valores negativos, para establecer este valor deberá borrar DiasHistoricoCubo del registro ya que así se usará el valor por defecto que es precisamente -1.*
    - 0: indefinido.
    - N: N días.
- REG_DWORD **DiasHistoricoDocumento**: número de días que se conservarán los documentos (por defecto 0).
    - 0: indefinido.
    - N: N días.
- REG_DWORD **ImportBlockLen**: tamaño de los bloques de registros que se irán habilitando durante la carga (por defecto 0).
    - 0: no se habilitarán los registros hasta que termine el proceso de carga.
    - N: número de registros.
- REG_DWORD **ImportFirstBlockLen**: tamaño del primer bloque de registros que se habilitarán durante la carga (por defecto 0).
    - 0: no se habilitarán los registros hasta que termine el proceso de carga.
    - N: número de registros.
- REG_DWORD **MaxIntentosTarea**: número máximo de intentos para realizar una tarea (por defecto 5).
- REG_DWORD **PollingInterval**: segundos de espera para una nueva ejecución (por defecto 10).
- REG_DWORD **RunDbOptimize**: permite indicar si se ejecutará la tarea de optimización de la base de datos (por defecto 1).
    - 0: no.
    - 1: sí.

Si en el proceso de carga se habilitan los registros por bloques, esto implica que para cada bloque se calcularán los registros por segmentos, con lo que el proceso de carga tardará más en completarse, así que no es recomendable definir un tamaño de bloque pequeño.

12 DYNAMIC BUSINESS ROUTER

12.1 EVOROUTER DAEMON

Este módulo es el responsable de gestionar el enrutamiento de interacciones (llamadas, email, etc) entrantes de Evolution.

Actúa de intermediario entre la fuente de interacciones (switch, buzón de mail, WebService, etc) y Evolution Server escuchando peticiones y dialogando con Evoserver para encolar las interacciones y recibir instrucciones respecto qué hacer.

Es posible configurar, desde Manager, los conectores DBR que definen la fuente de interacción (por ejemplo, el buzón de mail) y su estrategia de enrutamiento asociada.

Desde Manager se pueden configurar distintas estrategias indicando directamente los datos de enrutamiento o la URL de un servicio web que los obtenga.

Adicionalmente, EvoRouter Daemon permite publicar un servicio web (WebService API) que implementa los métodos públicos necesarios para permitir a aplicaciones externas la posibilidad de encolar, obtener información y desencolar interacciones no interactivas en EvoServer.

12.2 PARÁMETROS DEL SERVICIO

Se puede modificar su configuración por defecto a través de claves del registro de sistema, los parámetros principales son los siguientes:

12.2.1 CONFIGURACIÓN DEL SERVICIO

En la clave: **HKEY_LOCAL_MACHINE\SOFTWARE\ICR\EvoRouterDaemon**

- REG_SZ **ServerIpAddress**: dirección IP del servidor Evolution (por defecto 127.0.0.1).
- REG_DWORD **ServerPort**: puerto misceláneo del servidor Evolution (por defecto 3777).
- REG_DWORD **ResponseTimeout**: valor en milisegundos del timeout para espera de respuestas de Evoserver (por defecto 2000).
- REG_SZ **DefaultExtension**: extensión de la cola por defecto.
- REG_SZ **StrategyKey**: campo por el cual se indexarán las estrategias para interacciones interactivas. Valores aceptados: “DNIS”, “ROUTEPOINT” (por defecto “ROUTEPOINT”)
- REG_SZ **DBRScriptUrlBase**: raiz de la URL de las aplicaciones de Script (por defecto "http://localhost/Evolution/DBRScripts/").
- REG_SZ **DbConnectionString**: cadena de conexión con la base de datos Evolution(por defecto "DSN=EVOLUTIONDB;UID=NCADMIN;PWD=ADMN1cr@;").
- REG_SZ **DbDocConnectionString**: cadena de conexión con la base de datos de documentos Evolution(por defecto "DSN=EVOLUTIONDBDOC;UID=NCADMIN;PWD=ADMN1cr@;").
- REG_DWORD **TmrPop3Interval**: valor en segundos del intervalo de conexión a buzones de mail POP3 (por defecto 60).
- REG_DWORD **TmrDBRConnectorManagerInterval**: valor en segundos del intervalo de refresco del listado de conectores DBR (por defecto 60).
- REG_SZ **LogFile**: archivo de trazas (por defecto EvoTaskDaemon.log)

- REG_DWORD **MaxLogNum**: máximo número de archivos de trazas (rotativo) (por defecto 10).
- REG_DWORD **LogBytes**: tamaño máximo de los archivos de trazas (por defecto 10000000)
- REG_DWORD **LogLevel**: nivel de detalle de las trazas, los valores válidos van desde 0: máximo detalle, hasta 5: sin trazas (por defecto 1).
- REG_DWORD **WriteLogToFile**: indica si se han de guardar las trazas en fichero si(1) o no(0) (por defecto 1).

12.2.2 EN INTERACCIONES INTERACTIVAS, ¿CÓMO CONFIGURAR EVOROUTER PARA QUE SELECCIONE LA ESTRATEGIA POR DEFECTO A PARTIR DEL DN DEL ROUTEPOINT?

Edite la clave: **HKEY_LOCAL_MACHINE\SOFTWARE\ICR\EvoRouterDaemon**

- REG_SZ **StrategyKey**: “ROUTEPOINT”

En caso de no existir la clave **StrategyKey** se toma el valor por defecto “ROUTEPOINT”.

12.2.2.1 EN INTERACCIONES INTERACTIVAS,¿CÓMO CONFIGURAR EVOROUTER PARA QUE SELECCIONE LA ESTRATEGIA POR DEFECTO A PARTIR DEL DNIS DE LA LLAMADA?

Edite la clave: **HKEY_LOCAL_MACHINE\SOFTWARE\ICR\EvoRouterDaemon**

- REG_SZ **StrategyKey**: “DNIS”

12.2.3 INSTALACIÓN DE VOCES ADICIONALES PARA FUNCIONALIDADES DE SINTESIS DE VOZ Y RECONOCIMIENTO DEL HABLA.

Para las funcionalidades de síntesis de voz y reconocimiento del habla Evolution usa la plataforma Mirosoft Speech 11.

Por defecto para sitesis de voz se instalan los Runtime Languages:

- MSSpeech_TTS_es-ES_Helena.
- MSSpeech_TTS_es-MX_Hilda.
- MSSpeech_TTS_en-US_ZiraPro.

Estos permiten realizar sintesis de voz para las culturas es-ES, es-MX y en-US.

Por defecto para reconocimiento del habla se instalan los Runtime Languages:

- MSSpeech_SR_es-ES_TELE.
- MSSpeech_SR_es-MX_TELE.
- MSSpeech_SR_en-US_TELE.

Estos permiten realizar reconocimiento del habla para las culturas es-ES, es-MX y en-US.

Adicionalmente usted puede instalar Runtime Languages adicionales descargándolos desde el site de Microsoft:
http://www.microsoft.com/en-us/download/details.aspx?id=27224
Tenga en cuenta que los ficheros cuyo nombre empieza por MSSpeech_SR refieren a reconocimiento del habla. Y los ficheros cuyo nombre empieza por MSSpeech_TTS refieren a síntesis de voz.

13 DEVELOPER SERVICE

Este módulo se encarga de desplegar los scripts de aplicación de agente y los DBR Scripts, junto con las locuciones asociadas a DBRScripts en el servidor Asterisk configurado.

Las opciones a configurar están relacionadas con el despliegue de DBR Scripts, por lo que únicamente es necesario modificar los parámetros en el caso de que se vaya a usar este tipo de estrategias.

Para configurar los parámetros tendrá que modificar el archivo web.config del directorio de instalación de Developer Service (por defecto: C:\inetpub\wwwroot\Evolution\DeveloperService). En la sección <appSettings> configure las siguientes claves:

```
<!-- Parametros SFTP para audios de Script DBR -->
<add key="SFTPHost" value="scm" />
<add key="SFTPUser" value="evolution" />
<add key="SFTPPort" value="22" />
<add key="SFTPPassword" value="bomber" />
<!-- Directorio raiz donde se ubicarán las locuciones de los DBRScripts  -->
<add key="SFTPRootSounds" value="/var/lib/asterisk/sounds" />
<!-- Directorio raiz donde se gestiona Music on hold -->
<add key="SFTPRootMoh" value="/etc/asterisk"/>
<!-- Directorio fuente donde se encuentran los Scripts DBR -->
<add key="DBRScripts" value="Evolution/DBRScripts"/>
<!-- Puerto AMI para hacer el reload (el host es igual que el SFTPHost) -->
<add key="AMIPort" value="5038"/>
<!-- Usuario AMI -->
<add key="AMIUser" value="evolution"/>
<!-- Password AMI -->
<add key="AMISecret" value="bomber"/>
```

Para habilitar la reproducción en Asterisk de los archivos de música en espera de los DBR Script desplegados debe incluir el archivo **icr/icr.moh.conf** en el archivo de configuración de Music on hold de Asterisk.

Se trata del archivo **musiconhold.conf** o **musiconhold_custom.conf** en función de la distribución Asterisk que disponga. Ambos archivos se encuentran en el directorio SFTPRootMoh.

Añada por tanto la siguiente línea en musiconhold_custom.conf o en musiconhold.conf:

```
#include icr/icr.moh.conf
```

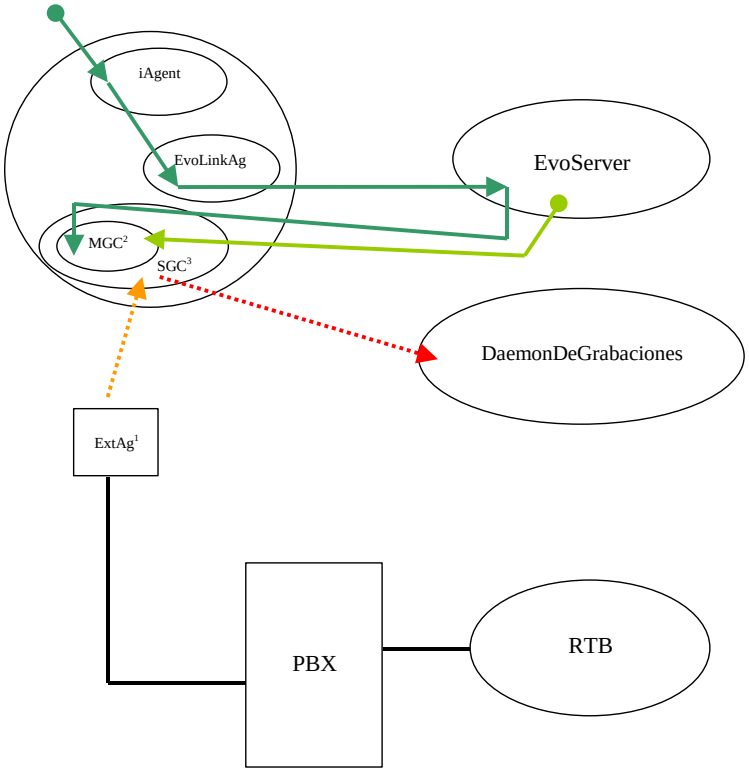
14 MÓDULO GRABADOR

Evolution es compatible con 3 tipos de grabaciones:

- ICR: es independiente de la marca y modelo de centralita, así que debería poder funcionar con cualquier tipo de centralita. El audio se debe extraer de los auriculares y pasarlo a la tarjeta de sonido del PC del agente, para ello se puede utilizar un adaptador.
- Nice: con esta integración Evolution puede gobernar el start/stop de las grabaciones *Nice*, así como etiquetar las grabaciones desde los argumentarios. *El software de grabación Nice debe ser proporcionados por el fabricante.*
- Asterisk: con esta integración Evolution puede gobernar el start/stop de las grabaciones si se usa Asterisk como centralita de telefonía.

14.1 ESQUEMA GENERICO

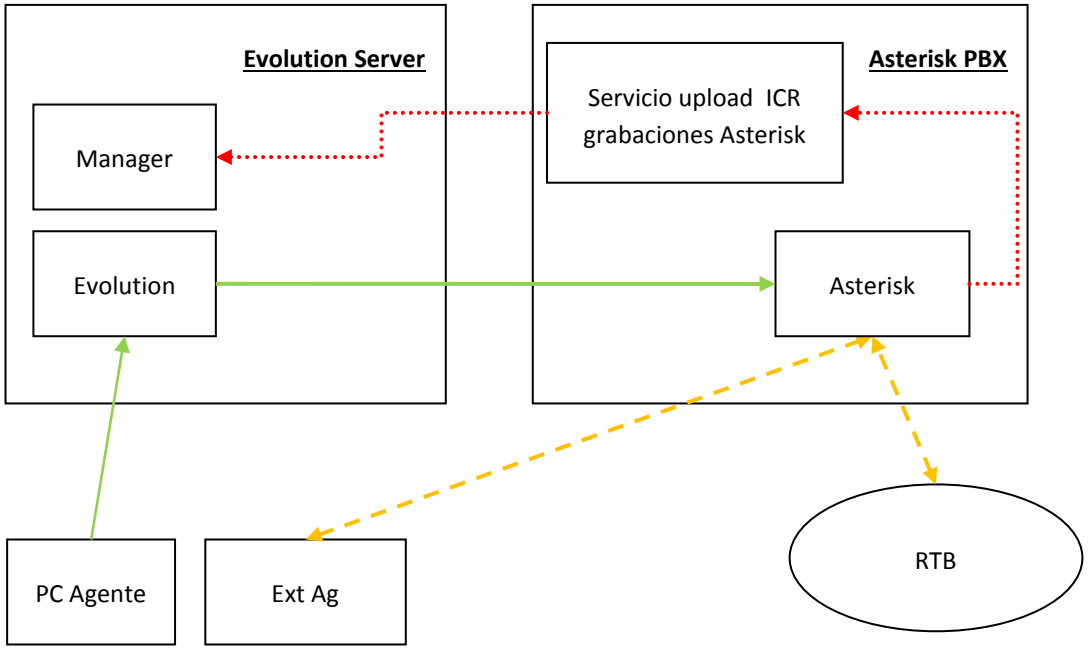
14.1.1 GRABADOR ICR (RECORDER DAEMON)



A petición del agente (campañas con grabación a demanda del agente o del argumentario) o a petición del servidor (campañas con grabación automática) el modulo MGC obtiene el audio digitalizado del auricular y lo codifica y almacena en formato .wav en disco duro local.

Posteriormente este archivo se envía automáticamente al daemon de Grabaciones (DDG), que lo almacena en el disco duro o sistema de almacenamiento de alta capacidad del servidor.

14.1.2 GRABADOR ASTERISK



A petición del agente (campañas con grabación a demanda del agente o del argumentario) o a petición del servidor (campañas con grabación automática) se le ordena a Asterisk que grabe la conversación.

Posteriormente desde el servidor Asterisk el servicio de upload para grabaciones que se proporciona con Evolution envía automáticamente las grabaciones a Evolution Manager, que lo almacena en el disco duro o sistema de almacenamiento de alta capacidad del servidor.

14.2 REQUERIMIENTOS CAPACIDAD DE ALMACENAMIENTO

El espacio utilizado es función del tipo de codificación utilizado.

Por ejemplo, en grabaciones ICR EvoMGC.Dll codifica el audio en un formato mp3. Y con los valores por defecto el bitrate utilizado es de 118 kBytes ·minuto = 6.9 Mbytes·hora

Bit rate= 118kBytes·minuto, 6,9 MBytes·hora

Ejemplo: jornada 12 horas (9 a 21) x 20 puestos agente, grabando un 50% del tiempo:

- 120 horas de grabación al día
- 6,9 x 120 = 828MB de grabación al día
- 25,6 GB al mes (31 días)

Por ejemplo, en grabaciones Asterisk, por defecto el audio se almacena en formato wave PCM lineal 8khz, 16 bits mono (stereo opcional). El bitrate resultante es de 8 khz x 16 bits = 128 kbits.segundo = 16kBytes•segundo = 56 MBytes·hora.

Bit rate= 16 kBytes·segundo ≈ 56 MBytes·hora

Ejemplo: jornada 12 horas (9 a 21) x 20 puestos agente, grabando un 50% del tiempo:

- 120 horas de grabación al día
- 56 x 120 = 6720MB ≈ 6,5 GBytes de grabación al día
- 201 GBytes al mes (31 días)

Por ejemplo, si en el servidor asterisk se usa una compresión a GSM 06.10 entonces el bitrate será de 13 kb·s

Bit rate= 13 kb·segundo = 46800 kb·hora = 5850 kBytes·hora ≈ 5,7 MB·hora

Ejemplo: jornada 12 horas (9 a 21) x 20 puestos agente, grabando un 50% del tiempo:

- 120 horas de grabación al día
- 5,7 x 120 = 685MBytes ≈ 0,7 GBytes de grabación al día
- 21,7 GBytes al mes (31 días)

14.3 ALTA DE UNA INSTANCIA DE GRABADOR EN MANAGER

Para cada servidor de grabaciones que instale debe generar una entrada de configuración en Manager.

Para un grabador **ICR** debe definir:

- El nombre del grabador. Ej: “CALIDAD”
- Dirección IP o nombre IP de la maquina y el puerto TCP donde escucha el daemon de grabadores (el mismo que se defina en el Daemon). Ej: 3663

Para un grabador **Nice** debe definir:

- El nombre del grabador. Ej: “GR_NICE”
- Dirección IP o nombre IP de la maquina y el puerto TCP donde escucha el daemon de grabadores para la integración con Nice. Ej: 3662
- Identificador de la centralita conectada al NICE.

Para un grabador **Asterisk** debe definir:

- El nombre del grabador. Ej: “GR_ASTERISK”

Valores de Puertos por defecto		
Modulo	Descripción	Puerto tcp/ip
Daemon RecorderServer	Grabador ICR MP3	3663
Daemon RecorderServer	Integración NICE	3662

*Los siguientes pasos a seguir para poder realizar grabaciones son:

- Asignar el grabador a los puestos deseados: en el apartado de Manager>Administración>Puestos al crear o editar puestos asignar el grabador que hemos creado en el punto anterior, esto se puede hacer para los puestos que se desee.
- Asignar el modo de grabación de la Campaña: en el apartado de Manager>Administración>Campañas al crear o editar la campaña se debe poner el campo "grabadores" de "SIN MARCACIÓN" a "Manual" por ejemplo.

Si se usa el softphone que está integrado en iAgent no se requiere crear ningún tipo de grabador.

14.4 NOTAS TÉCNICAS GRABADOR ICR

14.4.1 PROCESO DE INSTALACIÓN MANUAL DE IAGENT:

- Instalar iAgent
- Registrar EvoMGC.ocx
- La aplicación Lame.exe debe estar en el path.

14.4.2 PROCESO DE INSTALACIÓN MANUAL DEL MÓDULO SERVIDOR

El módulo servidor **DaemonRecorder.ocx** se instala con EvoConnector como cualquier otro Daemon Evolution.

```
evoconnector -instalar nombreservicio=RecordingServer
descripcion="Servidor Grabaciones"
```

14.4.3 ENVÍO DE GRABACIONES OFF-LINE

Si la aplicación iAgent se detiene, el envío de ficheros de audio continuará la siguiente vez que se ejecute.

Por defecto el directorio temporal de ficheros de audio del modulo grabador cliente (MGC) es C:\Documents and Settings\<USUARIO>\Local Settings\Temp\EvoMgc.

Si se produce una situación de error permanente que impide el envío de un archivo, esta situación se marcará generándose un archivo *.bad en el directorio de audio. El .WAV se mantendrá sin borrarse:

- audio en un archivo nombrado con el idContacto, la fecha y un número aleatorio y extensión ".wav"
- marca en un archivo con nombre idContacto, la fecha y un número aleatorio y extensión ".bad".
- Ej: 1000021309_20100830T150025_123.wav,1000021309_20100830T150025_123.bad.

Condiciones de error permanente pueden ser las siguientes:

- Error al convertir .wav a .mp3
- Idcontacto erróneo
- El archivo .mp3 no existe o ha sido borrado antes de su envío.

14.4.4 PARÁMETROS DEL DAEMONRECORDER (MÓDULO SERVIDOR)

El módulo servidor DaemonRecorder.ocx almacena los siguientes parámetros en la rama HK_LM/software/icr/daemonrecorder del registry:

- Global / RecordPath - Directorio local donde almacenara las grabaciones (Defecto: C:\icr\server\manager\audio). Este directorio debe coincidir con el directorio físico “audio” que se debe crear en el IIS dentro del directorio virtual MANAGER.
- Global / PortTcp : Puerto por donde se reciben los audio desde los EvoMGCs. (Defecto: 3663). Este parámetro también se debe configurar en Manager.
- BdD / DSN : Dsn de conexión a la base de datos. (Defecto: EVOLUTIONDB)
- BdD / User : Usuario de la base de datos (Defecto: NCADMIN)
- BdD / Password : Password de la base de datos (Defecto: ADMN1cr@)
- BdD / Owner : (Defecto: "")
- BdD / Prefix : (Defecto: “”)
- BdD / MaxErrors : (Defecto: 5)

14.4.5 PARÁMETROS DEL MÓDULO MGC (AGENTE)

El módulo agente MGC almacena los siguientes parámetros en la rama HK_LM/software/icr/evomgc del registry:

- Global / AudioPath: Directorio donde se guardan las grabaciones (Defecto Directorio temporal Temp o Tmp del sistema)
- Global / BitRate: Bitrate mp3 (Defecto: 16)
- Global /Frequency : Frecuencia de muestreo (Defecto: 12)

Se recomienda **no modificar los valores proporcionados por defecto**. Tener en cuenta que esta configuración es especifica del puesto, y afecta exclusivamente a las grabaciones de este puesto.

Hay que tener en cuenta también que los valores de BitRate y Frequency son dependientes entre si y que el aumento de estos provoca un aumento también del espacio en disco ocupado por cada grabación. Los valores posibles son:

- **Frequency** (KHz):

  8, 11.025, 12, 16, 22.05, 24, 32, 44.1, 48

- **BitRate**:

  Para frecuencias de muestreo de 32, 44.1 y 48 kHz:

  32, 40, 48, 56, 64, 80, 96, 112, 128, 160, 192, 224, 256, 320

  Para frecuencias de muestreo de 16, 22.05 y 24 kHz:

  8, 16, 24, 32, 40, 48, 56, 64, 80, 96, 112, 128, 144, 160

  Para frecuencias de muestreo de 8, 11.025 y 12 kHz:

  8, 16, 24, 32, 40, 48, 56, 64

14.5 NOTAS TÉCNICAS GRABADOR ASTERISK

14.5.1 REQUISITOS EN EL SERVIDOR EVOLUTION

Este tipo de grabación requiere que en el Servidor Evolution esté instalado ActivaTSP-1.4.9 o superior.

14.5.2 PROCESO DE INSTALACIÓN SCRIPTS PARA ASTERISK COMO SERVICIO

Para el correcto funcionamiento de las Grabaciones Asterisk con Evolution se requiere la instalación de unos scripts en el servidor Asterisk para la compresión y envío de las grabaciones al servidor Evolution. En este apartado le explicaremos como instalar estos scripts y configurarlos para que se ejecuten como servicio en su servidor Asterisk.

Los scripts para Asterisk proporcionados requieren tener instaladas las siguientes herramientas de línea de comandos:

- curl
- lame (para configuraciones de compresión de grabaciones en formato mp3)
- sox (para configuraciones de compresión de grabaciones a en formato vorbis)

Los scripts se proporcionan con el instalador de EvoServer, los puede encontrar en el servidor que haya instalado Evolution: DIRECTORIO_INSTALACION_EVOLUTION\addons\ICRRecUpScriptsForAsterisk.tar.gz

Para realizar la instalación de los scripts en su Asterisk, debe realizar el siguiente procedimiento como usuario root	
1	Copie ICRRecUpScriptsForAsterisk.tar.gz en algún directorio de su servidor Asterisk. Por ejemplo en /root/ICRRecUpScriptsForAsterisk.tar.gz
2	Descomprima el fichero: tar –xvzf ICRRecUpScriptsForAsterisk.tar.gz
3	Mueva los ficheros de la carpeta descomprimida a /usr/sbin/ mv ICRRecUpScriptsForAsterisk/* /usr/sbin/
4	Configurar la URL de manager para los uploads editando el script /usr/sbin/ICRRecUpAll.sh sManagerURL="http://DIRECCION_SERVIDOR_EVOLUTION/manager"
5	Para que arranque el servicio de Upload de grabaciones automático en cada inicio del sistema añada la siguiente línea en /etc/rc.local antes del “exit 0”. rc.ICRRecDaemonUp start Nota: si lo prefiere puede configurar el sistema para que arranque el script como un “script de inicio”, con un soft link en el directorio de runlevel apropiado (/etc/rcX.d).

Los scripts instalados son los encargados de realizar la compresión y subir las grabaciones a Evolution Manager. El script verifica si hay una nueva grabación cada intervalo de tiempo (configurado en **ICRRecDaemonUp** sTInterval por defecto 30segundos). En el caso que encuentre al menos una grabación realiza la compresión, sube la grabación comprimida a Evolution Manager y elimina la grabación del servidor Asterisk.

Observe que una vez realizada la grabación esta no estará disponible en Evolution Manager hasta que el servicio no haya validado la existencia de una nueva grabación y haya realizado la compresión y subido la grabación comprimida correctamente.

14.5.3 DESCRIPCIÓN DE LOS SCRIPTS PARA ASTERISK

Con el proceso de instalación anterior se instalan los siguientes scripts:

- **rc.ICRRecDaemonUp** controlador de arranque y parada del servicio de uploads automáticos.
    - rc.ICRRecDaemonUp start arranca el daemon.

- rc.ICRRecDaemonUp stop para el daemon.
- rc.ICRRecDaemonUp restart reinicia el daemon.

- **ICRRecDaemonUp** servicio de uploads automáticos, encargado de revisar periódicamente si hay grabaciones pendientes de ser subidas, realizar la compresión y el upload a Evolution Manager.
  Los siguientes parámetros son configurables editando el propio script:
  - sTInterval : Intervalo entre intentos de revisión de grabaciones pendientes de envío, en segundos. Por defecto 30 segundos.
  - sTraceFile: Destino de las trazas.
    - fichero de destino, se imprimen las trazas en el fichero de destino. (ej. /var/log/ICRRecDaemonUP).
    - stdout, las trazas se imprimen por la salida estándar.
    - None, no se imprimen trazas.

- **ICRRecUpAll.sh** script que al ser lanzado realiza la compresión y el upload de las grabaciones.
  Los siguientes parámetros son configurables editando el propio script:
  - sManagerURL: URL de Evolution Manager (ej. "http://host_evolution/manager").
  - sPrefix: prefijo a eliminar en el fichero de salida (ej. "icr").
  - sRecordingDir: Directorio de grabaciones asterisk (ej. "/var/spool/asterisk/monitor")
  - sTmpDir: Directorio temporal para realizar el transcoding (ej. "/tmp")
  - sInFormat: debe establecerse igual al formato en que se realizan las grabaciones. Los formatos soportados son los siguientes:
    - “wav” formato wav con codificación slin (signed linear)
    - “WAV” o “wav49” formato wav con codificación gsm
    - “ul” formato mu-law en bruto.
    - “al” formato a-law en bruto
    - “gsm” formato gsm en bruto
  - sOutFormat: Formato de las grabaciones que se subirán a Evolution Manager. I el formato de entrada es diferente al de salida, requiere la aplicación sox este instalada en el sistema Asterisk. Posibles formatos:
    - “wav” formato wav con codificación slin (signed linear) (128kbps)
    - “WAV” o “wav49” formato wav con codificación gsm (13kbps)
    - “wav-ul” formato wav con codificación mu-law (56kbps)
    - “wav-al” formato wav con codificación a-law (56kbps)
    - “mp3” requiere lame.
    - “ogg”
- **ICRRecUp.sh script** que realiza la compresión y upload de una grabación en concreto.
  El script requiere los siguientes argumentos:
  - Fichero de grabación.
  - Fichero temporal comprimido a generar.
  - URL de la página UploadAudio.aspx de Evolution Manager.

  Además editando el propio script puede editar los parámetros que usará lame o sox para realizar la compresión.

14.5.4 OTROS USOS DE LOS SCRIPTS PARA ASTERISK

Como se ha explicado en el apartado de “Proceso de instalación scripts para Asterisk como servicio”, pero en función de la carga del servidor Asterisk puede que no interese que la compresión de las grabaciones se realice una vez generada la grabación, ya que este proceso normalmente realiza un uso intensivo de la CPU.

Entonces puede que le interese dejar de usar los scripts como servicio y se realice la compresión y upload de las grabaciones en momentos de poca carga del servidor.

Por ejemplo para que se realiza la compresión y upload cada noche a las 22:00 se debería incluir la siguiente línea en el crontab:

```
00 22    * * * root /usr/sbin/ICRRecUpAll.sh
```

14.6 NOTAS TÉCNICAS GRABADOR NICE

14.6.1 CONFIGURACIÓN CERTIFICADA

La siguiente es la lista de equipos y software que se utilizó para la validación y certificación de Evolution en un entorno NICE PERFORM:

Equipamiento	Software
NICE Perform Server	NICE Perform R3 minimum SP4
NICE API	NICE Bridge, CLSAPI3Service
Evolution 10	Windows W2003 Server R2 32 bits SQL server 2008 Express

14.6.2 ARCHIVO DE CONFIGURACIÓN

La configuración de la integración con el servicio web NICE Bridge se encuentra en el archivo *EvoNiceClient.dll.config,* que está en la carpeta de instalación de Evolution.

Podemos dividir su contenido en dos partes:

1- Configuración de conexión al servicio web.
2- Mapeado de datos de negocio.

El archivo que tiene formato XML tiene el siguiente esqueleto:

```
<?xml version="1.0" encoding="utf-8"?>

<configuration>

        <system.serviceModel>

                ... (Conexión al servicio web) ...

        </system.serviceModel>

        <appSettings>
```

... (Mapeado de datos de negocio) ...

</appSettings>

</configuration>

14.6.3 CONEXIÓN AL SERVICIO WEB

El archivo se entrega con dos secciones en '*bindings'*: '*basicHttpBinding'* y '*netTcpBinding'*, dado que son las que soporta NICE Bridge.

También existen dos secciones en '*client'*, cada una asociada a uno de los '*bindings'*, deje únicamente el que corresponda al '*binding'* que va a utilizar. Además deberá ajustar la propiedad '*address'* que refleja la ubicación del servicio web para que apunte a su servidor (Dirección IP y puerto TCP, aunque se han incluido los puertos de la instalación por defecto).

La conexión al servicio web (*CLSAPI3*) se puede obtener con la herramienta *svcutil.exe (disponible en visual studio)*:

svcutil.exe /language:cs /out:generatedProxy.cs /config:app.config
http:///(ip del servidor):(puerto del servicio)/(servicio)

Esto nos generará entre otras cosas el archivo *app.config* que contiene los *endPoints* y *bindings* expuestos por el servicio web.

Esta información es la que se debe incluir en el archivo en la sección *<system.serviceModel>.*

Es **importante** que en la sección *<client>* sólo exista un *<endpoint.../>* ya que así la librería se conectará automáticamente a dicho *endPoint.*

14.6.4 MAPEADO DE LOS DATOS DE NEGOCIO

NICE permite 32 campos de negocio que tienen unas limitaciones:

Optional ID Field Numbers	Type	Maximum Size
3, 4, 9, 10, 11, 12	Number	N/A
1, 2, 13, 14, 15, 16	Text	20
7, 8	Text	30
5, 6, 17, 18, 19, 20, 21, 22	Text	40
23, 24, 25, 26, 27, 28, 29, 30	Text	80
31, 32	Text	120

A pesar de encontrarse indizadas, estas marcas son accesibles a través de la interfaz del servicio web por medio de la etiqueta con la que se definen.

Se deben crear los campos apropiados en la base de datos para almacenar las marcas (campos de negocio).

Existe un mapeado configurable en el archivo *EvoNiceClient.dll.config* que nos permite relacionar estos índices con los campos de negocio creados (*esta asociación es sensible a las mayúsculas).*

La sección *<appSettings>* contiene la definición del mapeado de negocio, aquí para cada campo creado se debe definir la entrada correspondiente añadiendo líneas con el siguiente formato:

<add key="C(índice del campo)" value="(nombre del campo)" />

p.ej.: <add key="C14" value="DNI" />

NOTA: hay que tener cuidado con el nombre, ya que es sensible a las mayúsculas.

14.7 CONFIGURACIÓN DEL NÚMERO DE THREADS POR GRABADOR

En caso de que NICE responda con lentitud a las peticiones, se puede incrementar el número de threads que gestionan las peticiones.
En la clave *[HKLM]\Software\ICR\EvoServer\Recorder* del registro de Windows el siguiente valor de tipo DWORD:
NumRecProc nos permite indicar el número de threads que atenderán a cada grabador (el número de peticiones que se podrán procesar en paralelo).
Dado que las peticiones llegan por el coordinador y se quedan esperando una respuesta, lo ideal es incrementar el coordinador en tantos threads como se indiquen en este nuevo parámetro.

15 SECURIZACIÓN DE LAS COMUNICACIONES

Es posible securizar o encriptar las comunicaciones a través de HTTPS (HTTP con cifrado SSL/TLS) de los siguientes elementos:

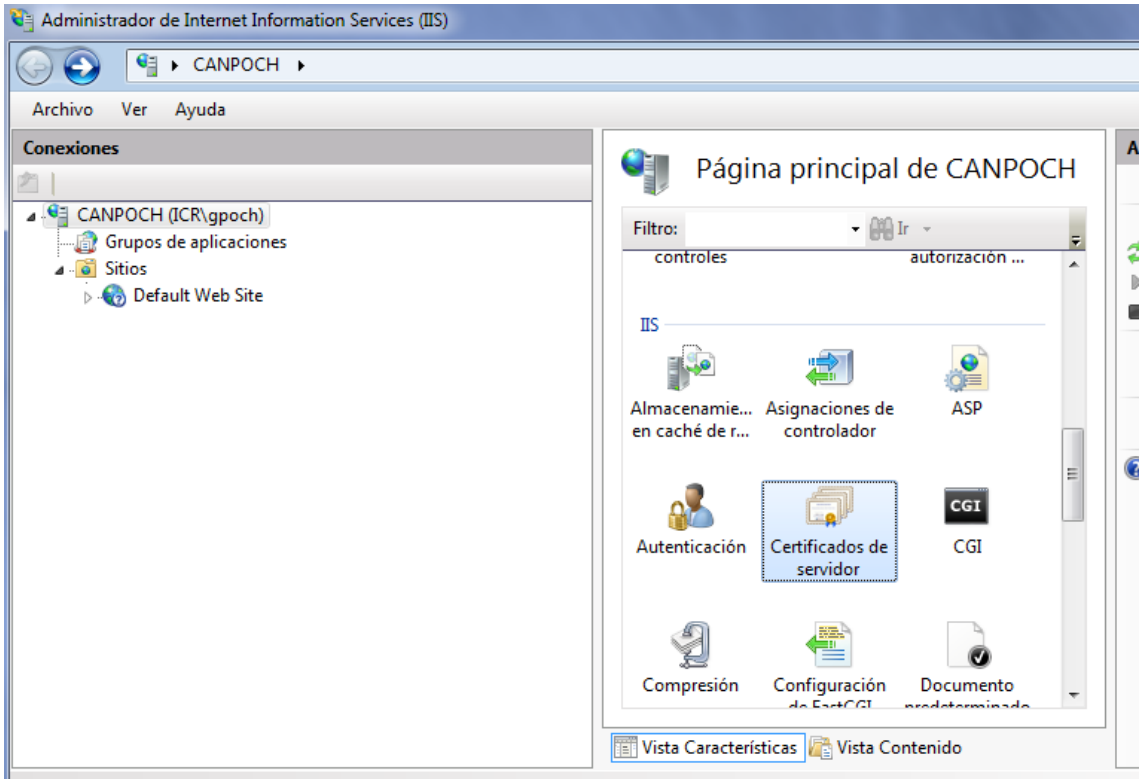
- Aplicación Manager
- Aplicación iAgent
- Argumentarios y páginas de sistema Evolution
- Despliegue de aplicaciones con Developer.NET (Developer Web Service Deploy)
- Evolution WebChat

15.1 ¿CÓMO PUBLICAR UNA APLICACIÓN VÍA HTTPS EN IIS?

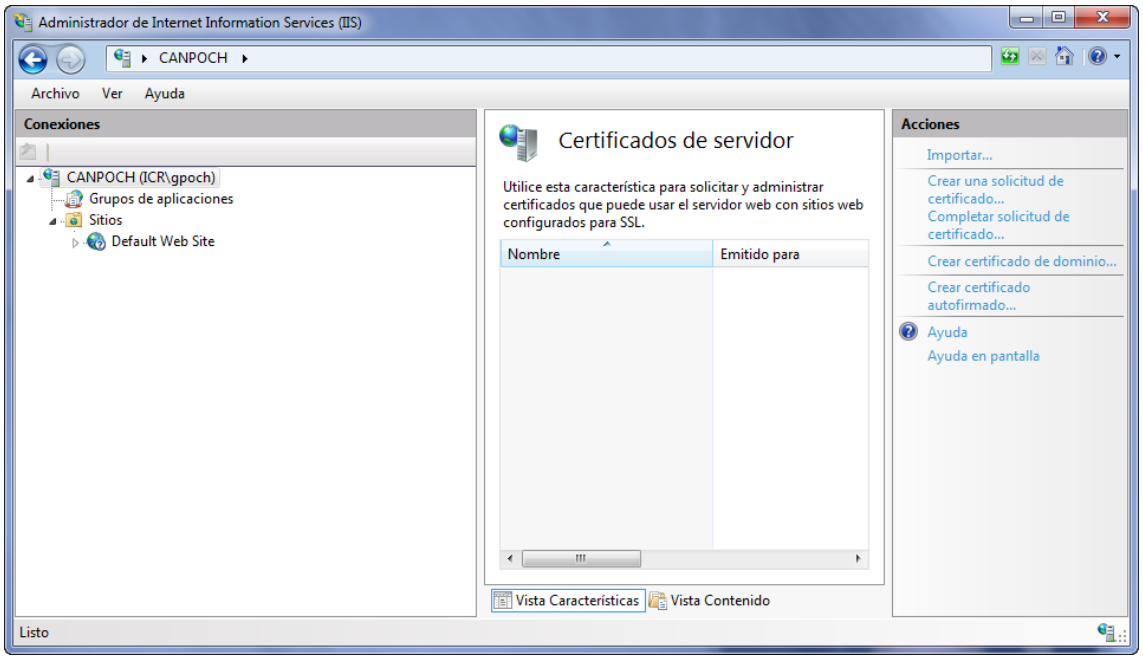
Para poder publicar las aplicaciones de Evolution en HTTPS, necesitaremos instalar un certificado digital en el servidor IIS que publica las aplicaciones de Evolution. El certificado digital puede obtenerse de alguna entidad emisora de certificados externa o, alternativamente, podemos crear nuestro propio certificado digital.

En este manual vamos a documentar esta última opción.

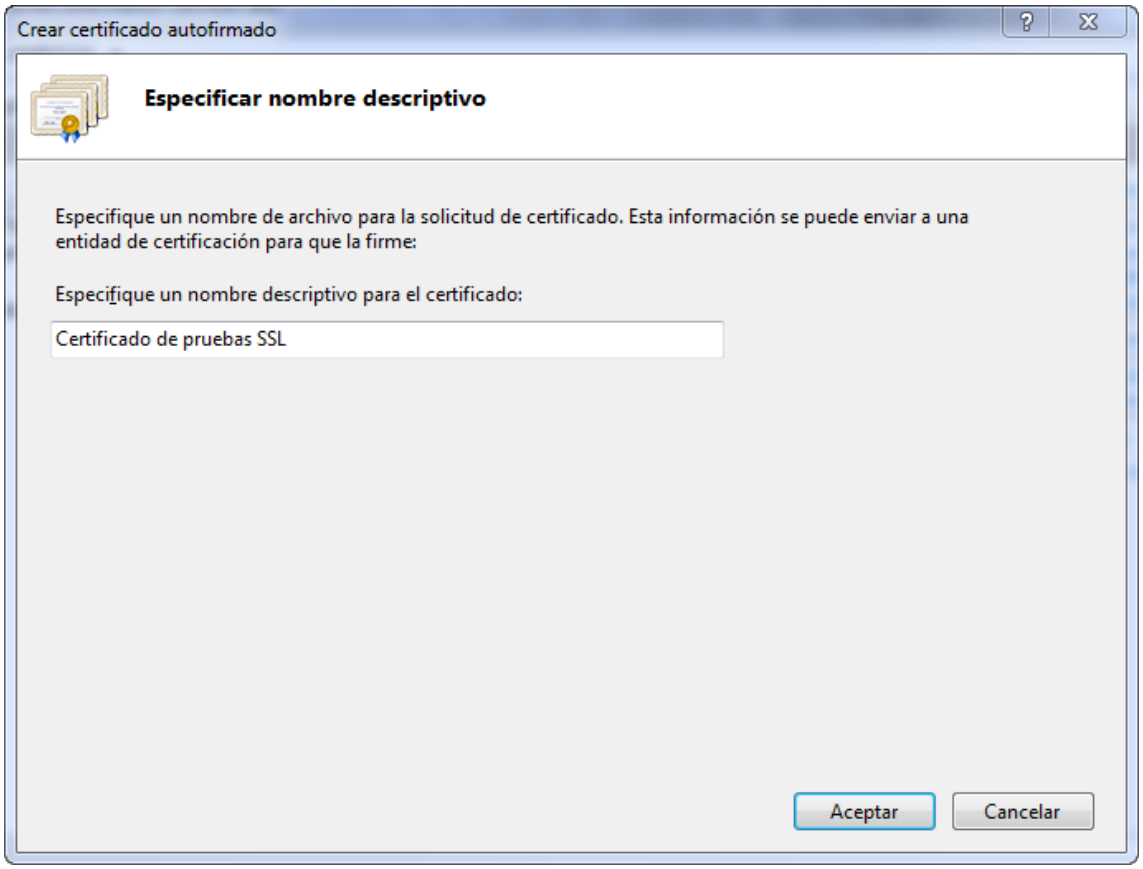
1) Crear un certificado de servidor autofirmado. Desde el Administrador de IIS, elegir la opción de “Certificados de servidor”

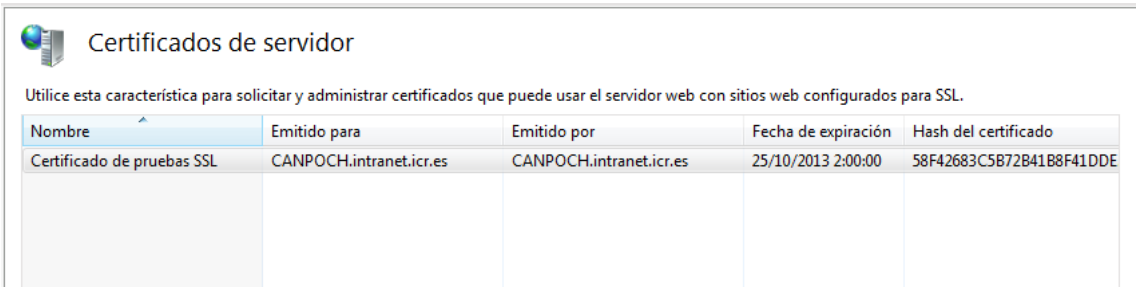


2) Escoger la opción “Crear certificado autofirmado…”



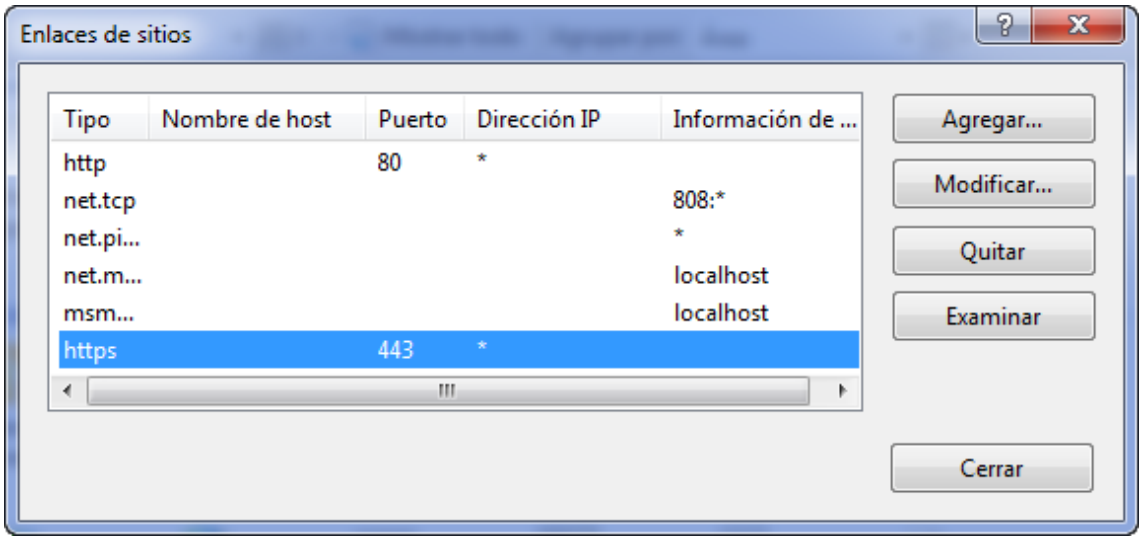
3) Especificar un nombre descriptivo del certificado a generar


Crear certificado autofirmado
Especificar nombre descriptivo
Especifique un nombre de archivo para la solicitud de certificado. Esta información se puede enviar a una entidad de certificación para que la firme:
Especifique un nombre descriptivo para el certificado:
Certificado de pruebas SSL
Aceptar
Cancelar



Nota: el certificado recién creado expira 1 año después de la fecha de creación. Crear un certificado digital con campos "a medida" queda fuera del ámbito de este manual.

4) Crear un enlace https para el Default Web Site. Desde el administrador IIS, seleccionar "Default Web Site" y elegir la opción "Enlaces…":

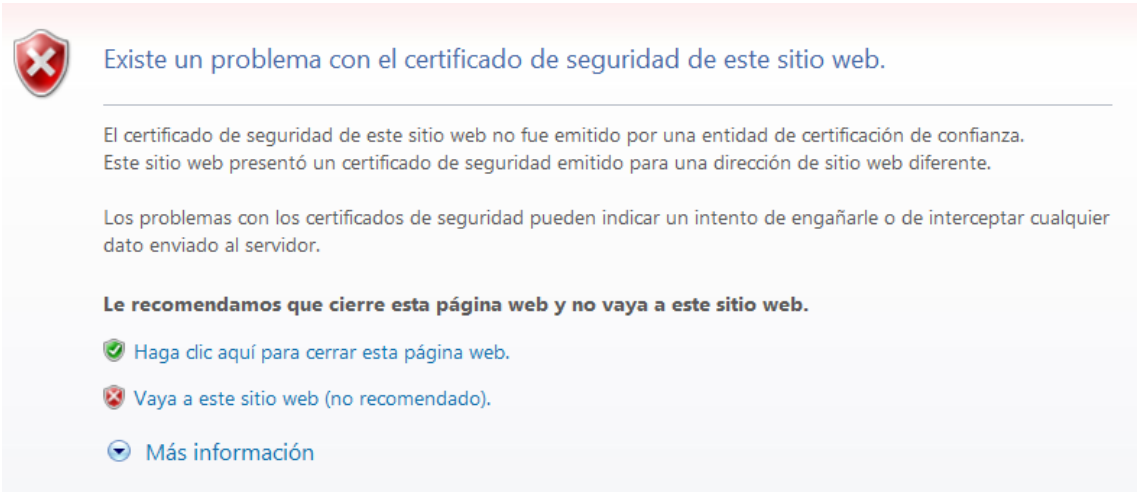


Agregar el enlace https al puerto por defecto (443) usando el certificado digital que acabamos de crear. A partir de este momento, deberíamos poder acceder a las aplicaciones IIS tanto por HTTP como por HTTPS.

Para ello, navegamos a una aplicación (por ejemplo, Manager) especificando el protocolo https. Por ejemplo: https://ip_del_servidor_Evolution/Manager.

NOTA: Es posible que el navegador muestre los siguientes avisos:

- **Este sitio web presentó un certificado de seguridad emitido para una dirección de sitio web diferente**. Realmente este error se produce cuando en la dirección del navegador hemos especificado un nombre diferente al certificado digital que acabamos de generar. Podemos especificar el nombre concreto (Ver el campo "Emitido para" del punto 3) o bien ignorar el error y pulsar "Vaya a este sitio web (no recomendado)".
- **El certificado de seguridad de este sitio web no fue emitido por una entidad de certificación de confianza**. Esto es debido a que el certificado ha sido firmado por una autoridad de certificación que no es de confianza (nosotros mismos). Podemos evitar este error añadiendo el certificado a la lista de entidades de certificación raíz de confianza del navegador o, como en el caso anterior, ignorando el error y pulsando "Vaya a este sitio web (no recomendado)".

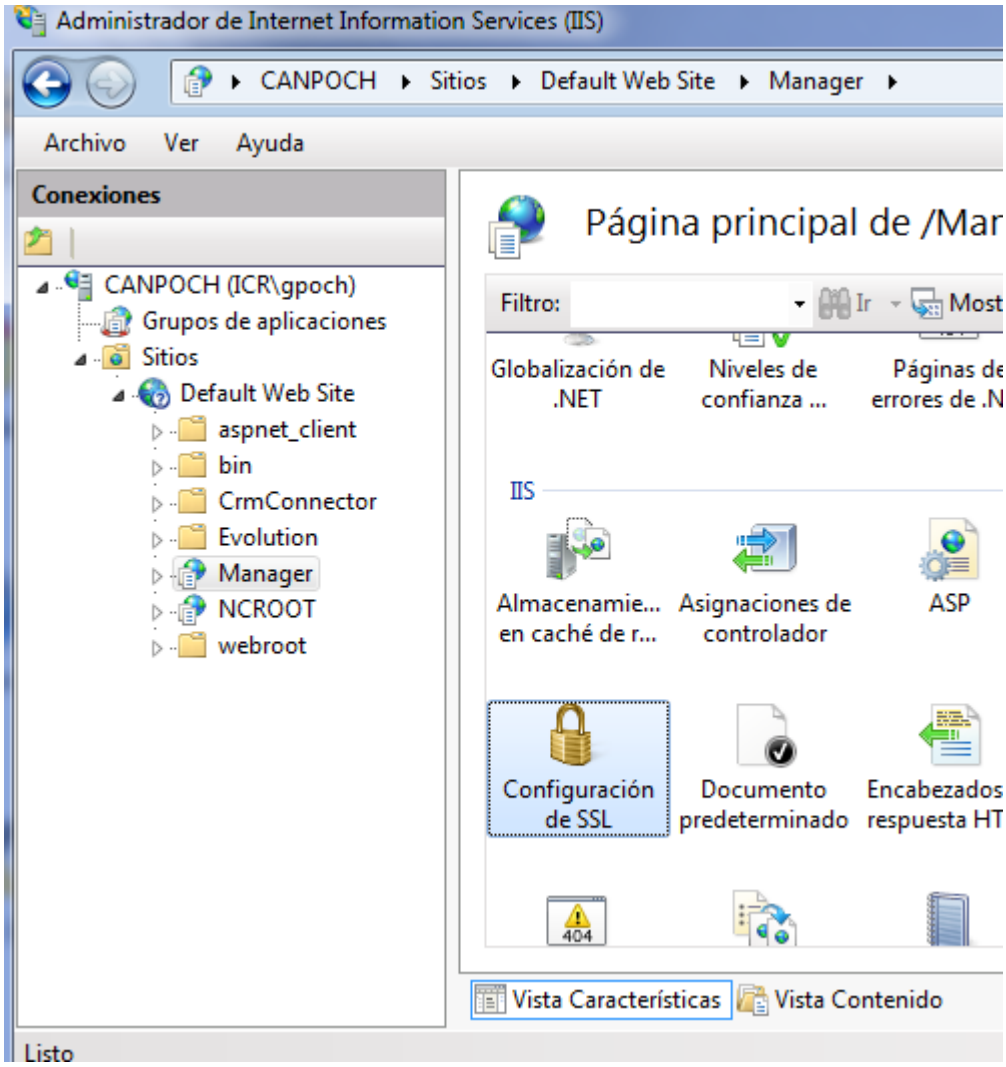

Existe un problema con el certificado de seguridad de este sitio web.
El certificado de seguridad de este sitio web no fue emitido por una entidad de certificación de confianza.
Este sitio web presentó un certificado de seguridad emitido para una dirección de sitio web diferente.
Los problemas con los certificados de seguridad pueden indicar un intento de engañarle o de interceptar cualquier dato enviado al servidor.
Le recomendamos que cierre esta página web y no vaya a este sitio web.
Haga clic aquí para cerrar esta página web.
Vaya a este sitio web (no recomendado).
Más información

Observe que en la línea de direcciones de Internet Explorer aparece un candado, indicando que se trata de un protocolo seguro:

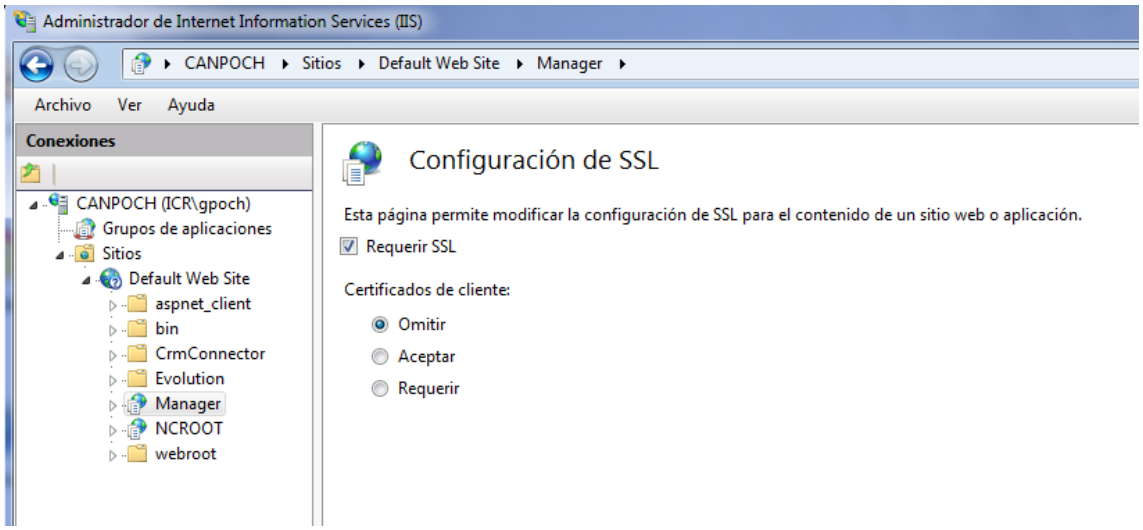
15.2 MANAGER

Siguiendo los pasos anteriores debe haber podido publicar Manager en HTTPS. Ahora sólo queda evitar que esta aplicación sea accedida por HTTP.

1) Desde el Administrador de IIS, seleccionar la aplicación “Manager” y elegir la opción “Configuración de SSL”



2) Marcar la opción “Requerir SSL” y “Omitir certificados de cliente”



A partir de este momento, Manager únicamente podrá ser accedido vía HTTPS.

15.2.1 GRABACIÓN INTEGRADA ASTERISK / SIP CALL MANAGER

Tenga en cuenta que si utiliza Asterisk o Evolution SIP Call Manager, y usa HTTPS en Manager, tendrá que adaptar la URL de subida de audios en el archivo/usr/sbin/ICRRecUpAll.sh, tal y como se indica en Proceso de instalación scripts para asterisk como servicio.

sManagerURL="https://DIRECCION_SERVIDOR_EVOLUTION/manager"

15.3 SECURIZACIÓN DEL ACCESO IAGENT MEDIANTE SSL (STUNNEL)

Las aplicaciones de agente se comunican con el servidor Evolution Server mediante un protocolo basado en XML/TCP. Puede encapsular este protocolo en SSL, encriptando las comunicaciones.

A continuación se detalla el procedimiento técnico para configurar un túnel SSL basado en stunnel.

15.3.1 ¿QUE ES STUNNEL?

“Stunnel es un programa de computadora libre multi-plataforma, utilizado para la creación de túneles TLS/SSL.

Stunnel puede ser utilizado para proveer conexiones cifradas seguras para clientes o servidores que no utilizan TLS o SSL de forma nativa. Corre en una gran variedad de sistemas operativos, incluyendo a la mayoría de los basados en el sistema operativo Unix y a la familia Windows. Su funcionamiento se basa en una biblioteca independiente como puede ser OpenSSL o SSLeay para implementar el protocolo TLS o SSL de capas inferiores.

Stunnel utiliza criptografía de clave pública con el certificado digital X.509 para asegurar la conexión SSL.”

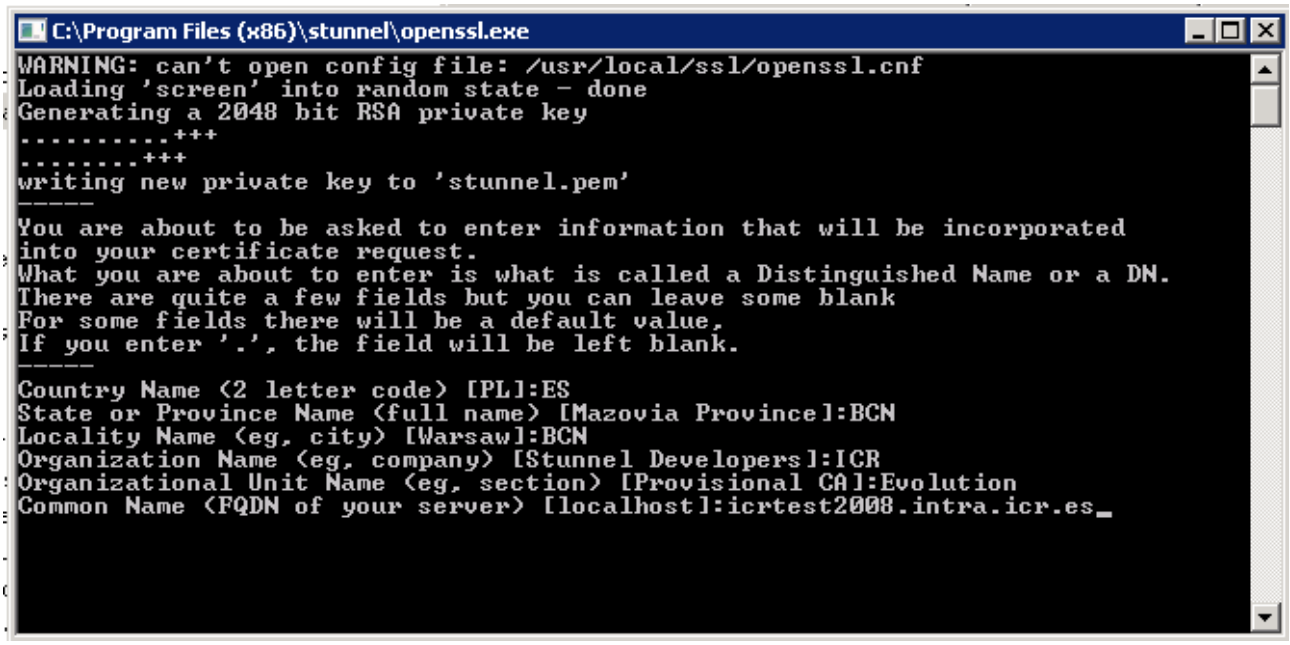
Para obtener más información y descargar el paquete, vea https://www.stunnel.org

15.3.2 CÓMO INSTALAR STUNNEL EN EL SERVIDOR EVOLUTION

1- Descargue el paquete stunnel y cópielo en el servidor Evolution.
   a. Acceda a https://www.stunnel.org/downloads.html
   b. Descargue el paquete `stunnel-4.56-installer.exe` y cópielo en el servidor Evolution
2- Ejecute el paquete instalador de stunnel 4.56 setup. En la página de selección de los componentes a instalar (“installation options”) puede dejarlos todos seleccionados.
   a. En todo caso, asegurese que los siguientes elementos están seleccionados para su instalación:
      i. “stunnel core files (requiered)”
      ii. “self-signed certificate tolos”
      iii. “start menú shorcuts”
3- Puede aceptar el “installation folder” por defecto
4- El proceso de instalación abrirá una ventana de comandos (command, ventana DOS), y se ejecutará la herramienta de `openssl.exe` para la generación de certificados auto-firmados.

Con esta herramienta vamos a poder generar un certificado de servidor auto-firmado para el servidor SSL. Si requiere otro tipo de certificado puede seguir las instrucciones que encontrará en http://www.stunnel.org

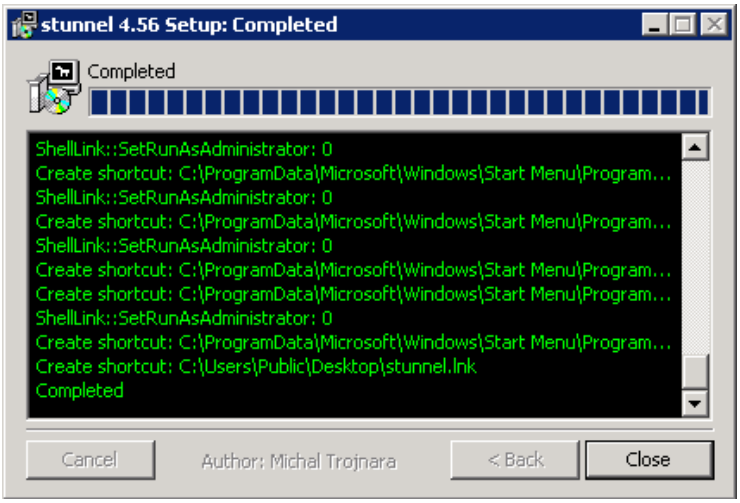
5- Paragenerar el certificado autofirmado continuaremos entrando los datos que nos requiere la herramienta. Introduzca los datos. Por ejemplo:
   a. Country Name (2 letter code)= ES
   b. State or Province Name: BCN
   c. Locality Name: BCN
   d. Organization Name: ICR
   e. Organizational Unit Name: Evolution
   f. Common Name: icrtest2008.domainname.com


C:\Program Files (x86)\stunnel\openssl.exe
WARNING: can't open config file: /usr/local/ssl/openssl.cnf
Loading 'screen' into random state - done
Generating a 2048 bit RSA private key
.....+++
.....+++
writing new private key to 'stunnel.pem'

You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.

Country Name (2 letter code) [PL]:ES
State or Province Name (full name) [Mazovia Province]:BCN
Locality Name (eg, city) [Warsaw]:BCN
Organization Name (eg, company) [Stunnel Developers]:ICR
Organizational Unit Name (eg, section) [Provisional CA]:Evolution
Common Name (FQDN of your server) [localhost]:icrtest2008.intra.icr.es

6- El proceso de instalación continuará, revise que se ejecuta correctamente, hasta el final y sin errores.



7- Instale stunnel como servicio Windows. Para ello acceda al “Menú de Inicio Windows”, “Todos los Programas”, “stunnel” y ejecute “stunnel Service Install”.
    a. Si usa configuración UAC deberá ejecutar dicho comando con la opción de botón derecho de ratón “ejecutar como administrador”
    b. Acceda al “panel de control Windows | herramientas administrativas | servicios locales” y compruebe que existe un servicio llamado “stunnel”

Ahora debemos establecer los parámetros de nuestro túnel.

El objetivo es establecer un túnel seguro entre el puerto estándar Evolution (por defecto: port 3555) y las aplicaciones de los agentes. Para ello debemos configurar stunnel para que abra un puerto de escucha SSL (por ejemplo accept = 35555) y lo conecte al puerto estándar evoserver (por ejemplo connect = 3555)

8- Para configurar los parámetros del túnel acceda al “Menú de Inicio Windows”, “Todos los Programas”, “stunnel” y ejecute “Edit stunnel.conf”.
9- Ubique el final del archivo Stunnel.conf, y añada una nueva sección [evoserver], con los siguientes parámetros:
    a. Accept = 35555
    b. Connect = 3555
10- Guarde los cambios y salga del editor

Stunnel.conf
[evoserver] accept = 35555 connect = 3555

11- Reinicie el servicio stunnel. Acceda al “panel de control Windows | herramientas administrativas | servicios locales” y seleccione el servicio stunnel. Reinicielo.

Con estos pasos hemos configurado stunnel para que establezca un puerto SSL de escucha (35555) y lo conecte al puerto estandar evoserver 3555.

Ahora deberemos configurar las aplicaciones de los agentes para que se conecten a dicho puerto mediante SSL.

En un puesto de trabajo en el que tenga correctamente instalado iagent.exe puede configurar el uso de SSL:

12- Acceda al dialogo de configuración de iagent.exe. Para ello:
    a. Acceda al menú Ayuda | Acerca de…
    b. Teclee la contarseña secreta “bomber”+<ENTER>, lo cual abrirá el diálogo de “configuración”
    c. Pulse el botón “Configurar enlace…” para acceder al dialogo “Propiedades de EvoLink Agent Control”
13- En este dialogo “Propiedades de EvoLink Agent Control” edite
    a. TCP Port=35555

b. Use SSL = yes
c. Guarde los cambios con Aceptar

14- Reinicie la aplicación iagent.exe para que los cambios surtan efecto

15.3.3 NOTAS ADICIONALES SOBRE LA SEGURIDAD

Para mantener un alto grado de seguridad en el servidor puede ser necesario administrar el firewall Windows u otros firewalls para que impidan y bloqueen accesos por otros puertos no seguros.

Le recomendamos acuda al fabricante de su firewall para obtener las indicaciones y recomendaciones oportunas.

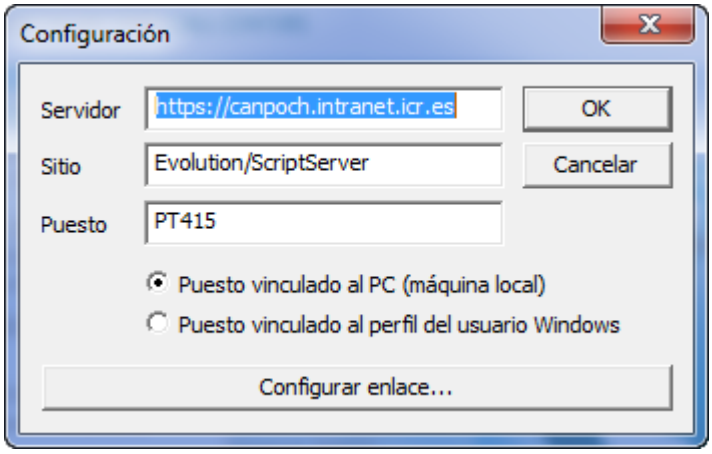
15.4 ARGUMENTARIOS Y PÁGINAS DE SISTEMA DE EVOLUTION

Para hacer que las páginas de sistema y los argumentarios de Evolution sean accedidos por HTTPS, deberemos repetir los mismos pasos que para Manager (ver “15.2 Manager”) para la siguiente aplicación:

- Evolution/ScriptServer

Los argumentarios de Evolution se encuentran bajo este directorio y, por lo tanto, heredarán esta configuración. No es necesario por tanto repetir la operación para todas y cada una de las aplicaciones o argumentarios de agente.

Debemos configurar iAgent de los agentes del call center para que acceda en modo HTTPS:



15.5 SECURIZACIÓN DEL DESPLIEGUE CON DEVELOPER.NET

Para hacer que el despliegue de aplicaciones con Developer.NET funcione con SSL, hay que realizar los siguientes cambios:

En el servidor de Evolution:

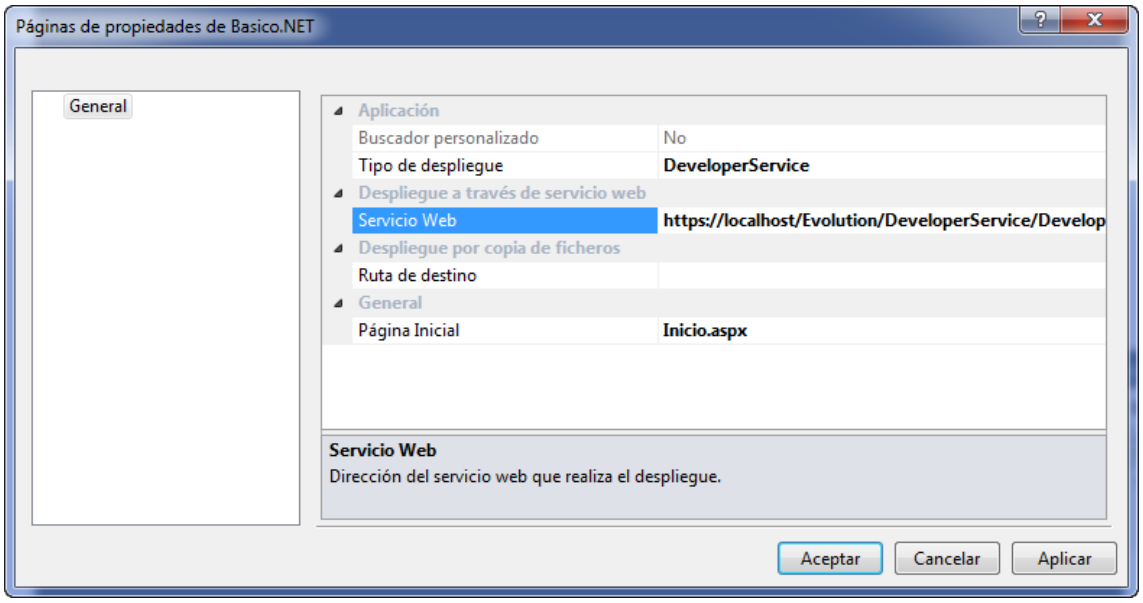
- Hacer que la aplicación /Evolution/DeveloperService requiera SSL (ver puntos anteriores).
- Modificar el web.config de /Evolution/DeveloperService para que únicamente admita despliegue por HTTPS:
  - Descomentar el endpoint para publicar en https
  - Comentar el endpoint para publicar en http
  - Hacer que el endpoint mex tenga binding **mexHttpsBinding** en lugar de mexHttpBinding.
  - En la sección behaviour activar httpsGetEnabled y desactivar httpGetEnabled

Con todo ello web.config debe quedar así:

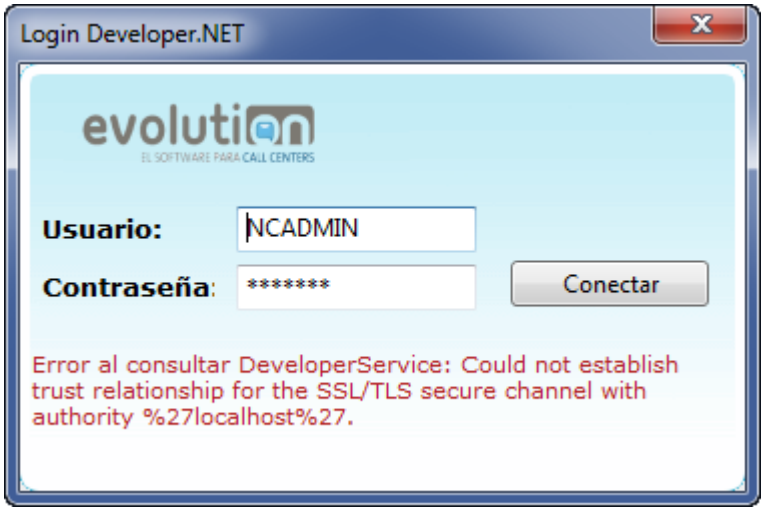
```
<system.serviceModel>
    <services>
      <service name="Icr.Evolution.Developer.DeveloperService.DeveloperService"
behaviorConfiguration="DeveloperService.DeveloperServiceBehavior">
        <!-- Service Endpoints -->

        <!-- Endpoint para publicar Developerservice en HTTPS (descomentar) -->
        <endpoint address="secure" binding="wsHttpBinding" bindingConfiguration="SFileTransferBinding"
contract="Icr.Evolution.Developer.DeveloperService.IDeveloperService">
          <identity>
            <dns value="localhost" />
          </identity>
        </endpoint>


        <!-- Endpoint para publicar DveloperService en HTTP
        <endpoint address="" binding="wsHttpBinding" bindingConfiguration="FileTransferBinding"
contract="Icr.Evolution.Developer.DeveloperService.IDeveloperService" />
                -->
        <!-- Para publicar Developerservice en HTTPS cambiar el binding a mexHttpsBinding -->
        <endpoint address="mex" binding="mexHttpsBinding" contract="IMetadataExchange" />
      </service>
    </services>
    <behaviors>
      <serviceBehaviors>
        <behavior name="DeveloperService.DeveloperServiceBehavior">
          <!-- To avoid disclosing metadata information, set the value below to false and remove the metadata
endpoint above before deployment -->
          <!-- Para publicar Developerservice en HTTPS poner httpGetEnabled="false" httpsGetEnabled="true" --
>
          <serviceMetadata httpGetEnabled="false" httpsGetEnabled="true" />
          <dataContractSerializer maxItemsInObjectGraph="200000000" />
          <!-- To receive exception details in faults for debugging purposes, set the value below to true.
Set to false before deployment to avoid disclosing exception information -->
          <serviceDebug includeExceptionDetailInFaults="false" />
        </behavior>
      </serviceBehaviors>
    </behaviors>
    <bindings>
      <wsHttpBinding>
        <binding name="SFileTransferBinding" closeTimeout="00:01:00" openTimeout="00:01:00"
receiveTimeout="00:10:00" sendTimeout="00:01:00" maxReceivedMessageSize="200000000">
          <!--70MB-->
          <readerQuotas maxArrayLength="200000000" />
          <security mode="Transport">
            <transport clientCredentialType="None" />
            <message clientCredentialType="None" negotiateServiceCredential="false"
establishSecurityContext="false" />
          </security>
        </binding>
        <binding name="FileTransferBinding" closeTimeout="00:01:00" openTimeout="00:01:00"
receiveTimeout="00:10:00" sendTimeout="00:01:00" maxReceivedMessageSize="200000000">
          <!--70MB-->
          <readerQuotas maxArrayLength="200000000" />
          <security mode="None">
            <transport clientCredentialType="None" />
```

```
        </security>
      </binding>
    </wsHttpBinding>
  </bindings>
</system.serviceModel>
```

Cuando queramos desplegar una aplicación con Developer.NET, en las propiedades del proyecto, Servicio Web, especificar el protocolo https en lugar de http:



NOTA: Si aparece el error

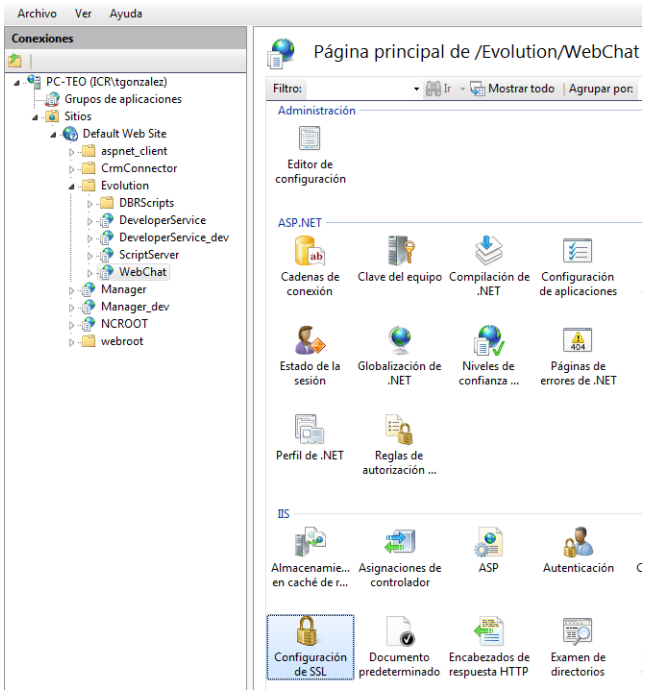


Revise que el nombre del servidor coincide con el campo “Emitido para” del certificado digital.

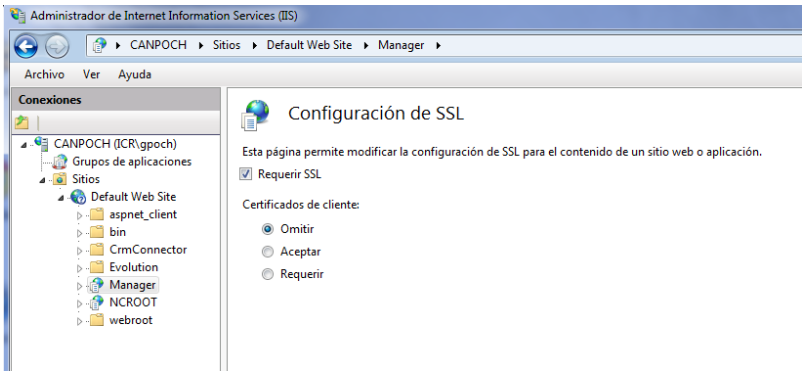
15.6 WEBCHAT

Siguiendo los pasos anteriores debe haber podido publicar WebChat en HTTPS. Ahora sólo queda evitar que esta aplicación sea accedida por HTTP.

1) Desde el Administrador de IIS, seleccionar la aplicación “WebChat” y elegir la opción “Configuración de SSL”



2) Marcar la opción “Requerir SSL” y “Omitir certificados de cliente”



A partir de este momento, WebChat únicamente podrá ser accedido vía HTTPS. Así pues, la llamada URL al punto de entrada a WebChat (*WebChat.aspx*) deberá realizarse haciendo uso del protocolo HTTPS.

Para hacer que Evolution WebChat funcione correctamente con SSL, hay modificar el web.config de WebChat para que únicamente admita despliegue por HTTPS. Para ello será necesario:

- Modificar el contenido de la sección behaviour para activar httpsGetEnabled y desactivar httpGetEnabled.
- Descomentar el endpoint para publicar en https

- Comentar el endpoint para publicar en http

Con todo ello el archivo web.config debe quedar similar a:

```
<system.serviceModel>
    <behaviors>
      <endpointBehaviors>
        <behavior name="eStreamChat.ChatEngineBehavior">
          <enableWebScript/>
        </behavior>
      </endpointBehaviors>
      <serviceBehaviors>
        <behavior>
          <serviceDebug includeExceptionDetailInFaults="True"/>
          <!-- Activar HTTP o HTTPS (sólo puede activarse uno)   -->
          <serviceMetadata httpGetEnabled="false" httpsGetEnabled="true" />
        </behavior>
      </serviceBehaviors>
    </behaviors>
    <serviceHostingEnvironment aspNetCompatibilityEnabled="true" multipleSiteBindingsEnabled="true"/>
    <services>
      <service name="eStreamChat.ChatEngine">
        <!-- Endpoint para publicar WebChat en HTTP  -->
        <!--<endpoint address="" behaviorConfiguration="eStreamChat.ChatEngineBehavior"
binding="webHttpBinding" bindingConfiguration="WebChatBinding" contract="eStreamChat.ChatEngine" />-->
        <!-- Endpoint para publicar WebChat en HTTPS  -->
        <endpoint address="" behaviorConfiguration="eStreamChat.ChatEngineBehavior" binding="webHttpBinding"
bindingConfiguration="SSLWebChatBinding" contract="eStreamChat.ChatEngine" />
      </service>
    </services>

    <bindings>
      <webHttpBinding>
        <!-- SSL WebChatBinding -->
        <binding name="SSLWebChatBinding">
          <security mode="Transport">
            <transport clientCredentialType="None" />
          </security>
        </binding>
        <!-- Non SSL WebChatBinding -->
        <binding name="WebChatBinding">
          <security mode="None">
            <transport clientCredentialType="None" />
          </security>
        </binding>
      </webHttpBinding>
      ...
```

16 ANEXO A: CONFIGURACIONES DE TELEFONÍA

Evolution server soporta un número de switch del mercado. A continuación se describen los procedimientos detallados para utilizar Evolution con las configuraciones más comunes.

Para otras configuraciones o switch, consultar con ICR.

16.1 AVAYA AURA COMMUNICATIONS MANAGER Y AES

Recomendado con TSAPI AES 5.x.

Evolution soporta los siguientes tipos de campaña con Avaya Aura Communications Manager y AES:

- Inbound switch based routing
- Outbound vp
- Outbound predictivo/progresivo

16.1.1 CONFIGURACIÓN CERTIFICADA

La siguiente es la lista de equipos y software que se utilizó para la validación y certificación de Evolution en un entorno AVAYA AES:

Equipamiento	Software
Avaya S8300D Media Server	Avaya Aura® Communication Manager 6.0 Service Pack 1 R016x.00.0.345.0 -18444
MM710AP	HW05 FW020
MM712AP	HW07 FW009
Dell 1950 Server	Avaya Aura® Application Enablement Services 5.2.2
Avaya 9600 Series telephones	H.323 Firmware 3.11
Avaya TSAPI Client For Windows32	5.2.1.474

Notas: Para los modos de marcación progresivo o predictivo, Evolution hace uso de la funcionalidad *MakePredictiveCall*. Según documentación de Avaya, esta funcionalidad requiere la licencia avanzada de AVAYA Aura AES TSAPI Advanced License.

16.1.2 CÓMO CONFIGURAR EL SERVIDOR TSAPI AES

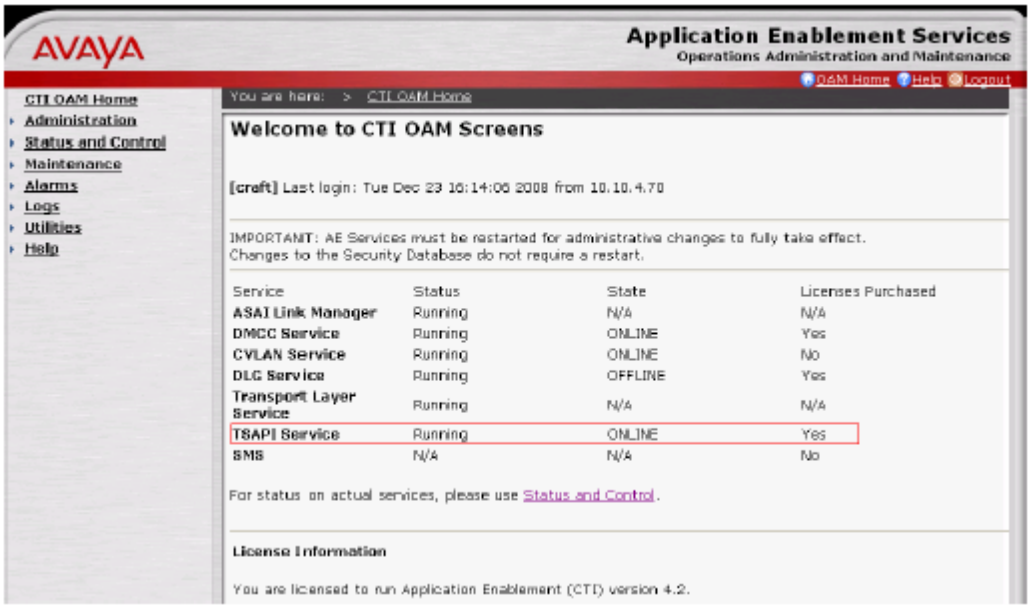
Este apartado describe los procedimientos para configurar *Avaya Application Enablement Services*. Los procedimientos contemplan las siguientes áreas:

1. Verificar las licencias Avaya Application Enablement Services
2. Administrar una “switch connection”
3. Administrar un “TSAPI link”
4. Habilitar un “CTI Link User”
5. Administrar Evolution user

16.1.2.1 VERIFICAR LAS LICENCIAS AVAYA AES

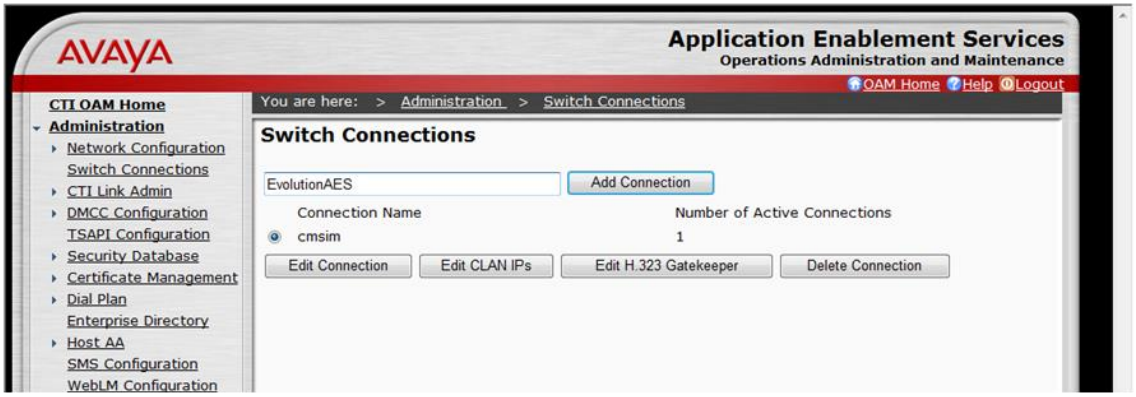
Inicializa la interfaz web AES OAM navegando a "http://x.x.x.x/MVAP/index.jsp", donde "x.x.x.x" es la dirección IP del AES, y identifícate (log-in).

Desde la pantalla "OAM Home" selecciona "CTI OAM Admin" para mostrar el menú "CTI OAM Home". Verificar que el servicio TSAPI está licenciado en la pantalla de "Welcome to CTI OAM", asegurándose que el "TSAPI Service" se encuentra en la lista de servicios de la sección de información de licencias.


AVAYA
Application Enablement Services
Operations Administration and Maintenance
OAM Home Help Logout
CTI OAM Home
Administration
Status and Control
Maintenance
Alarms
Logs
Utilities
Help
You are here: > CTI OAM Home
Welcome to CTI OAM Screens
[craft] Last login: Tue Dec 23 16:14:06 2008 from 10.10.4.70
IMPORTANT: AE Services must be restarted for administrative changes to fully take effect.
Changes to the Security Database do not require a restart.
Service Status State Licenses Purchased
ASAI Link Manager Running N/A N/A
DMCC Service Running ONLINE Yes
CVLAN Service Running ONLINE No
DLG Service Running OFFLINE Yes
Transport Layer Service Running N/A N/A
TSAPI Service Running ONLINE Yes
SMS N/A N/A No
For status on actual services, please use Status and Control.
License Information
You are licensed to run Application Enablement (CTI) version 4.2.

16.1.2.2 ADMINISTRAR UNA "SWITCH CONNECTION" AES

Desde el menú de "CTI OAM Home", selecciona **Administration → Switch Connections**. En la pantalla de "switch connections", selecciona **Add Connection**.

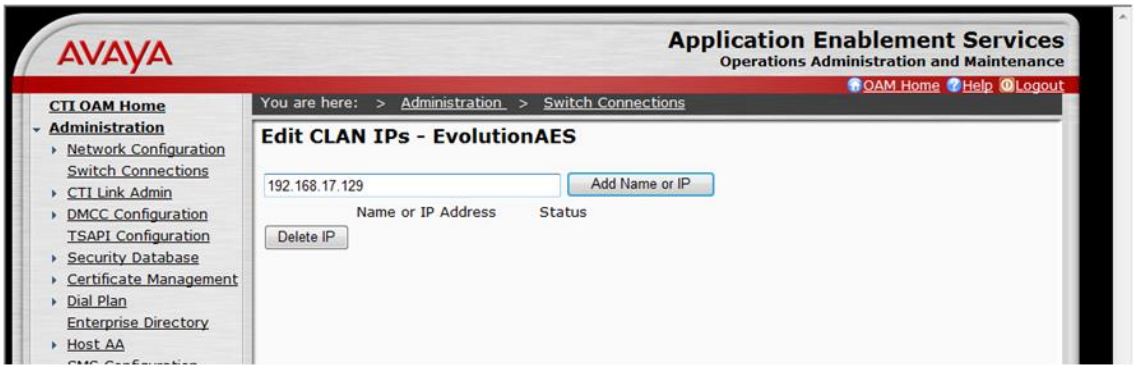


En la pantalla de “Add Connection”, entra los siguientes valores:

6. **Connection Name:** Elige un nombre para la conexión, como por ejemplo: “EvolutionAES”

Puede ser necesario que revises otros parámetros:

7. **Password:** Selecciona la contraseña para la conexión al switch
8. **Edit CLAN IPs:** Establece la IP de la CLAN que deberá utilizarse en esta conexión.



16.1.2.3 ADMINISTRAR EL TSAPI LINK

Desde el menú de “CTI OAM Home”, selecciona **Administration → CTI Link Admin → CTI Link Admin → TSAPI Links**. En la pantalla de “TSAPI Links”, selecciona **Add Link**. En la pantalla de “Add/Edit TSAPI Links”, entra los siguientes valores:

9. **Link:** Usa la lista desplegable para seleccionar un número d elink que esté libre. El número de link seleccionado es “1”.
10. **Switch Connection:** elige la conexión de switch “EvolutionAES”, que ha sido previamente configurada desde el desplegable.
11. **Switch CTI Link Number:** Correspondiente al número de “CTI link” configurado.
12. **Security:** Aquí seleccionamos **“**Unencrypted**”**.

Cuando termines, selecciona **Apply Changes**.

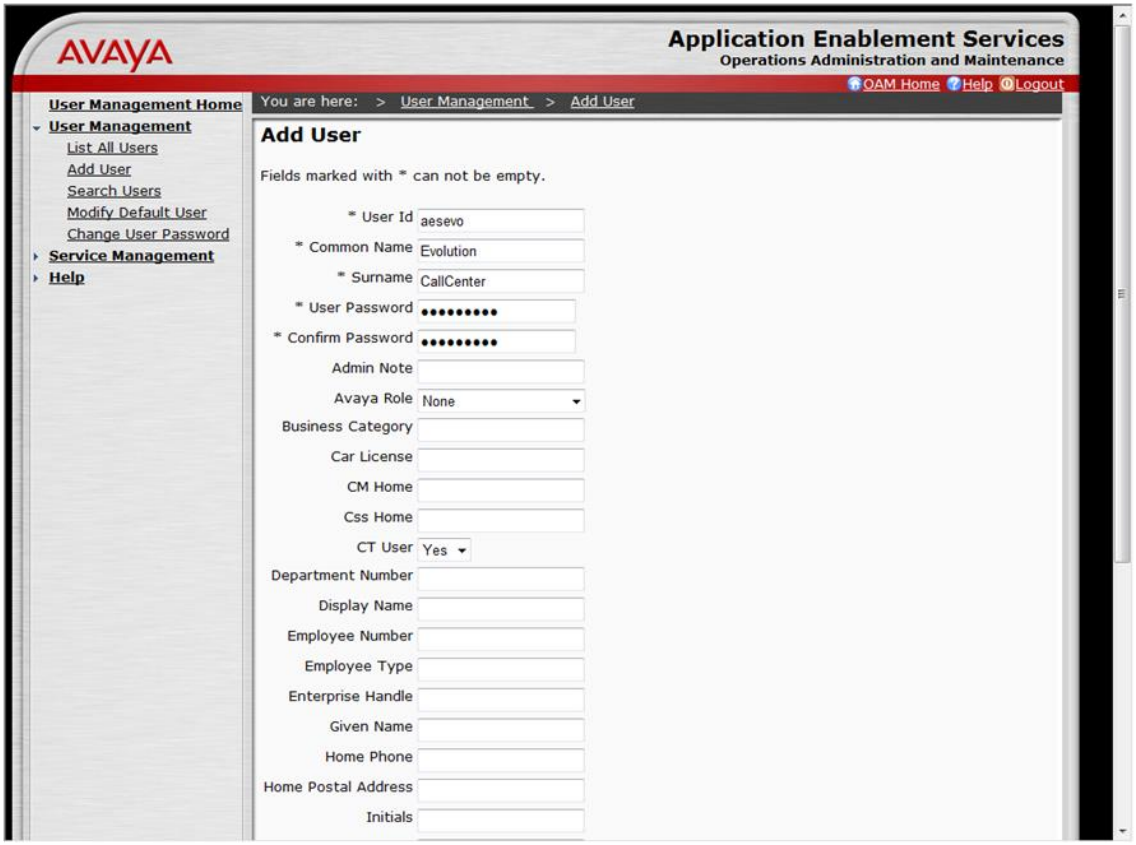
El AES debe ser reiniciado para que los cambios sean efectivos. Desde el menú “CTI OAM Home”, selecciona **Maintenance → Service Controller**. En la pantalla de control de servicios, selecciona **Restart AE Server**.

16.1.2.4 ADMINISTRAR UN USUARIO EVOLUTION

Se debe configurar un usuario y contraseña para que EVOLUTION se comunique como cliente TSAPI con el servidor AES. Accede a **OAM Home → User Management** y accede a las pantallas de “User Management”. Selecciona **User Management** y **Add User**. En la pantalla de **Add User**, entra los siguientes parámetros:

13. **User ID –** Este es el usuario que deberá ser utilizado por Evolution. Por ejemplo: “aesevo”
14. **Common Name and Surname –** Entra un nombre descriptivo.
15. **New Password and Confirm Password –** Esta es la contraseña que se utilizará conjuntamente con el “User Id”
16. **CT User –** Selecciona “Yes” del desplegable.

Completa el proceso seleccionando ‘Apply’ al final de la pantalla.

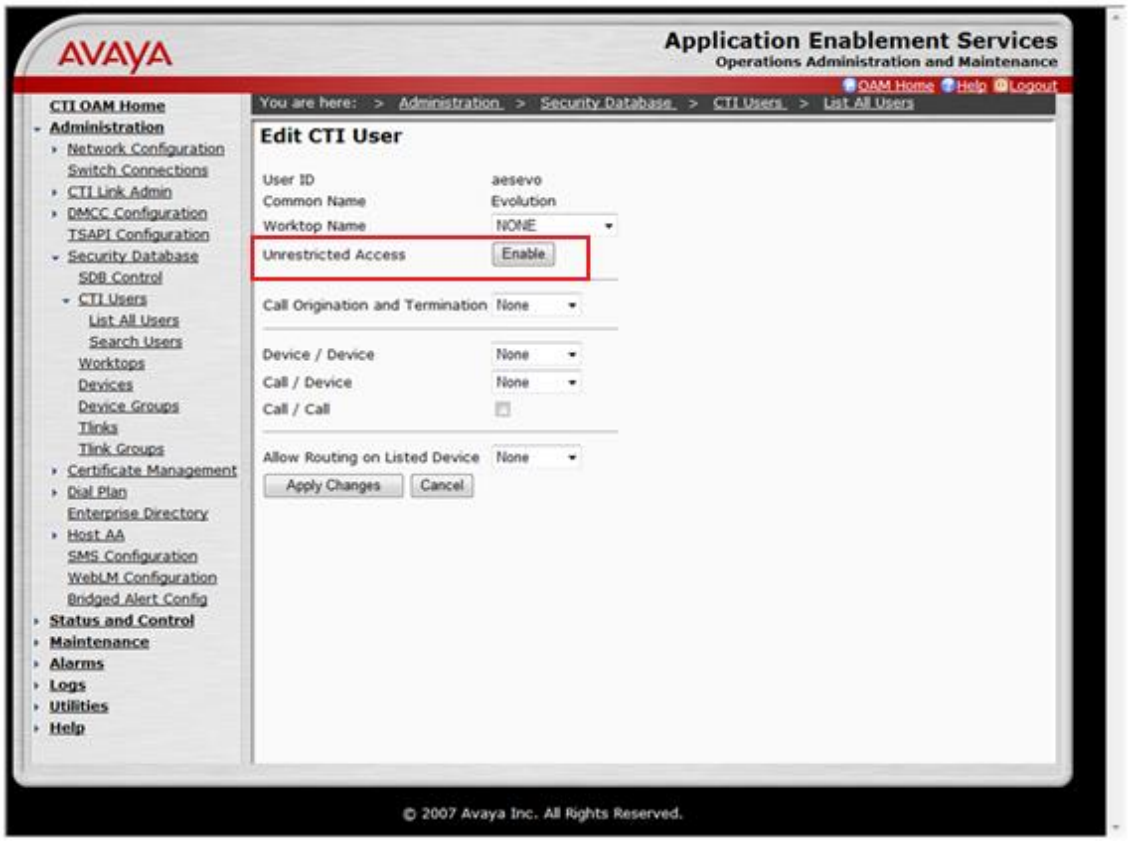


16.1.2.5 HABILITAR EL USUARIO DEL CTI LINK

Navega a “CTI Users” seleccionando CTI OAM Home → Administration → Security Database → CTI Users → List All Users.

Selecciona el usuario ‘aesevo’ que has preparado en el apartado anterior y selecciona la opción de “Edit”.

Selecciona el botón ‘Enable’ de la opción de “Unrestricted Access”, y ‘Apply Changes’ al final de la pantalla.



16.1.3 CÓMO INSTALAR EL CLIENTE TSAPI AES

Instala el componente "Avaya AES TSAPI Windows Client"[2] en el servidor Evolution.

Editar el archivo tslib.ini, mediante "Avaya AE Services | TSAPI client | Edit TSLIB.INI". En la sección [Telephony Servers], añade la entrada correspondiente al **Switch Connection que anteriormente se ha definido en AES server.** Por ejemplo: "EvolutionAES o "AESSIM"."

```
[Telephony Servers]

; This is a list of the servers offering Telephony Services via TCP/IP.

; Either domain name or IP address may be used; default port number is 450

; The form is: host_name=port_number   For example:

;

; tserver.mydomain.com=450

AESSIM=450
```

[2] Por ejemplo "Avaya Application Enablement (AE) Services TSAPI Windows Client Release 5.2.1"

16.1.4 CÓMO COMPROBAR EL CORRECTO FUNCIONAMIENTO DE TSAPI AES

Comprueba el correcto funcionamiento del conjunto AES server/client con la utilidad Avaya AE Services | TSAPI client | TSAPI Test.

Esta aplicación permite realizar una llamada entre dos extensiones, a través de TSAPI.

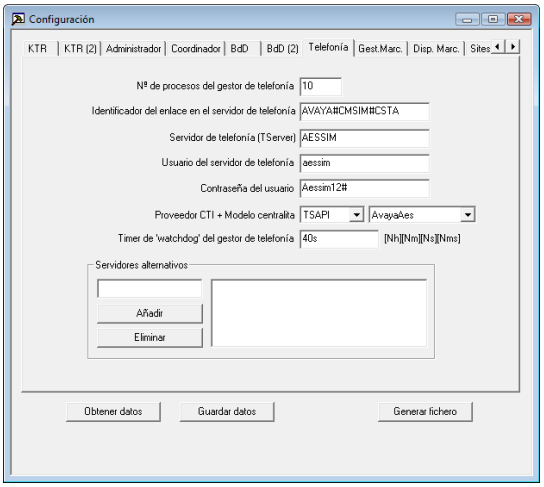
16.1.5 CÓMO CONFIGURAR EL ENLACE EVOLUTION AL SERVIDOR TSAPI AES

A través de Evoadmin.exe se deberán configurar los siguientes **parámetros de telefonía:**

Parametro	Valor	Ejemplos
Identificador del enlace en el servidor de telefonía	Tres primeros identificadores del “stream” TSAPI.	P.ej: “AVAYA#CMSIM#CSTA”
Servidor de telefonía Tserver	Especifica la localización del TSAPI, corresponde al cuarto identificador del “stream” TSAPI	P.ej: “AESSIM”
Usuario y contraseña del servidor de telefonía	Usuario AES TSAPI. Asegúrese de que ha definido este usuario en AES y que dispone de los privilegios necesarios.	Ej: aessim/ aessim
Proveedor CTI + Modelo centralita	TSAPI/AES o TSAPI/Definity	Ej: TSAPI / AES

Configuración de telefonía en evoadmin

Ejemplo de configuración en Evoadmin



16.1.6 CÓMO CONFIGURAR EL MÓDULO ICR DIALER DAEMON (EVODIALERSERVER)

Configuración del Servidor de Marcación con AVAYA usando "Call Classifier"

El termino **Call Classifier** se refiere a una funcionalidad AVAYA que permite clasificar las llamadas y determinar aquellas que se establecen positivamente.

1 Iniciar c:\ICR\Evolution\Server\DialerParam.exe

2 Indicar la Máquina donde está instalado el Servidor de Marcación y pulsar Obtener Datos.

Ej: "Maquina de Dialer": "." (un punto, indicando local)

3 En la pestaña DialerGlobal:

> **Module** escribir el número 69 que es el correspondiente al tipo TsapiAesGcc.

>**MainLinkID** escribir el mismo valor que hayamos indicado en el parámetro "Identificador del enlace en el servidor de telefonía" en evoadmin. P.ej: "AVAYA#CMSIM#CSTA"

>**MainServerID** nombre del servidor de telefonía. Escribir el mismo valor que hayamos indicado en el parámetro "Servidor de telefonía Tserver" en evoadmin.

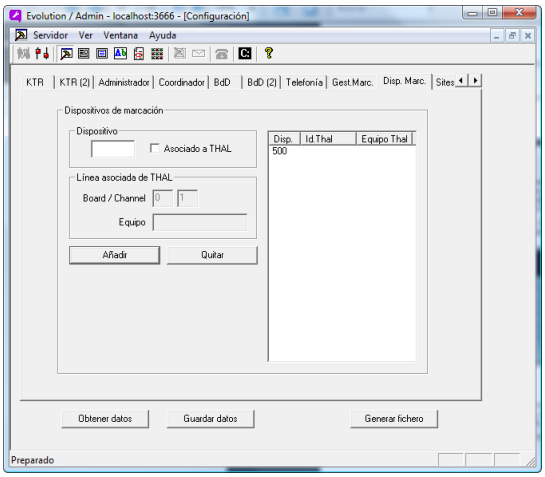
	P.ej: “AESSIM” >**MainLogin/MainPwd** usuario/contraseña. Escribir los mismos valores que hayamos indicado en los parámetros “Usuario y contraseña del servidor de telefonía”.. Ej: aessim/ aessim
4	Y pulsamos Guardar Datos.

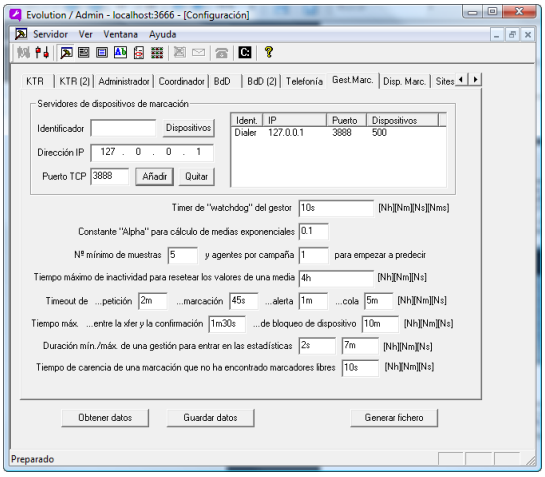
16.1.7 CÓMO ADMINISTRAR LOS DISPOSITIVOS DE MARCACIÓN EN EVOADMIN

En el caso de utilizar VDNs AVAYA CM, dichos dispositivos de marcación Evolution son dispositivos “lógicos”, y no corresponden a DN o dispositivos reales AVAYA.

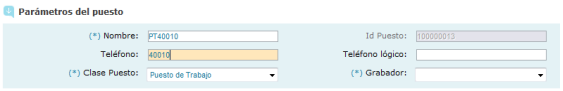
No obstante debe administrar un número suficiente y adecuado de dispositivos de marcación en Evoadmin, para soportar los procesos de marcacion.

Configuración de Dispositivos de Marcación en evoadmin

1	Ejecute evoadmin.exe, indique el *password* para operaciones restringidas, acceda al diálogo de “Configuración”, TAB “Disp. Marcador” y edite la lista de dispositivos de marcación. Para evitar confusiones y dado que estos dispositivos de marcación son “lógicos” y no corresponden a dispositivos reales en AVAYA, recomendamos que opte por una numeración de dispositivos que *no* coincida con dispositivos reales. Pulse Guardar Datos.	

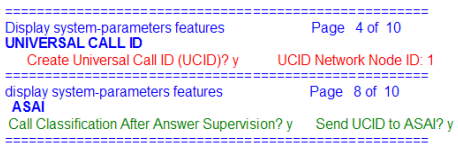
2	En el TAB “Gest. Marc.” pase a “off-line” el marcador seleccionando el identificador del “servidor de dispositivos de marcación” y pulsando el botón “Quitar”. Pulse “Dispositivos”, edite la lista de dispositivos añadiéndole todos los dispositivos correspondientes a wave ports. Una vez editados pulse “Añadir” para pasar a “on-line”. Pulse Guardar Datos.	

16.1.8 CONFIGURACIONES DE EVOLUTION MANAGER

	Configuración Manager	
1	Administración | Puestos	Informe el número de la extensión (STATION DN) en el parámetro “teléfono” Deje vacío el “teléfono lógico” Ej: teléfono: 40010 
2	Administración | Usuarios	Informe en los parámetros de ACD el “login ACD” y “password ACD” administrados en AVAYA. Cuando el agente Evolution se conecte, se utilizarán estos parámetros para efectuar el login AVAYA. Ej: Login ACD: 50001
3	Administración | Campañas	En la sección “Cola” seleccione la opción “switch-

		based” Evolution determina que las llamadas *inbound* pertenecen a una campaña cuando el `calleddevice` de la llamada coincide con el DN de una estrategia DNIS asociada a la campaña. Administre una o más estrategias de tipo DNIS, asociadas a la campaña. Administración, campañas, ver estrategias, y configure una o mas estrategias de tipo de encaminamiento ‘DNIS’, y asígnela a la campaña. Normalmente en Avaya el valor de DNIS debe coincidir con el VDN que entregue las llamadas a los agentes. Ej: Estrategia de encaminamiento tipo DNIS con DN: 100 y asociada a la campaña “atención al cliente” En la administración de campaña informe el parámetro “Disp. De control” con el VDN que deberá generar las llamadas predictivas/progresivas. Si la campaña no usa marcación progresiva o predictiva puede dejar este campo vacío. Ej: Disp. De control: 30001
4	Administración | Servicios	En una centralita Avaya las secuencias de conexión permiten activar o desactivar automáticamente skills al agente. Por ejemplo: ***25<LOGINACD>#401#1#** añade el agente al skill 401, con prioridad 1 ***24<LOGINACD>#401#** elimina agente del skill 401

16.1.9 NOTAS TÉCNICAS

Instalación y configuración de Avaya CM		
1	Activar Universal Call ID (UCIC) On page 4: Set UCID to Y, and assign an ID as well. On page 8: Verify Send UCID to ASAI to Y.	 Create Universal Call ID (UCID)? **Y = If set to Y, Definity will generate UCID for each call when necessary.** N = If set to N, Definity will not generate a UCID for any call. UCID Network Node ID: **You have to Enter a number unique to this server/switch in a network of switches.** Valid Entries = 1 to 32767 or Blank, this number is an important part of the UCID tag and must be unique to the server/switch.
2	En algunos casos el módulo AVAYA callclassifier puede clasificar erróneamente la llamada como POSITIVA inmediatamente, antes de que el cliente descuelgue, y esta llamada se ofrece al agente. Debe configurarse *Call Classification After Answer Supervision: yes*	**Call Classification After Answer Supervision: yes**
3	Para llamadas progresivas o predictivas, Evolution hace uso de la funcionalidad MakePredictiveCall. Según documentación de Avaya, esta funcionalidad se encuentra encapsulada bajo la licencia avanzada de TSAPI (TSAPI Advanced License).	

16.2 AVAYA IP OFFICE

Recomendado: TAPI / IPOFFICE TAPI3 SERVICE PROVIDER

Evolution soporta los siguientes tipos de campaña con Avaya IP Office:

- Inbound switch based routing
- Outbound vp
- Outbound predictivo/progresivo

Se requieren licencias AVAYA “IP Office CTI Link Pro”

Para los modos de marcación progresivo o predictivo, Evolution hace uso de usuarios funcionalidad WAVE-PORTS. Según documentación de Avaya, esta funcionalidad requiere el uso de licencias WAVE-PORTS.

16.2.1 CONFIGURACIÓN CERTIFICADA

La siguiente es la lista de equipos y software que se utilizó para la validación y certificación AVAYA DEVCONNECT de Evolution en un entorno AVAYA IPOffice:

Equipamiento	Software
Avaya IP OFFICE 500 v2	IP Office R7.0.23
Avaya 96xx H.323 Deskphone	Avaya H323 IP Office Firmware Ha96xxua3_Hbas.nin
Avaya 2420 Digital Sets	N//A
Avaya IP OFFICE TAPI3 client for Windows32	Tspi3w.tsp 1.0.0.17
Evolution 10.1	Windows W2003 Server R2 32 bits SQL server 2008 Express

16.2.2 ¿CÓMO GESTIONA EVOLUTION LAS EXTENSIONES DE LOS AGENTES?

- Evolution controla las extensiones correspondientes a los puestos de trabajo.
- Cuando un agente se conecte a Evolution a través de TAPI se enviará una secuencia correspondiente a USER-LOGIN, p.ej: “*35*123*456#”, donde 123 y 456 son el “login ACD” y “password ACD” del usuario Evolution. Estos valores deben corresponder con el usuario IPOffice y su password.
- Cuando el agente se desconecte de Evolution, si el usuario es el de por defecto, no se hará log-out. Si el usuario no es el usuario por defecto (hot desking user) se hará logout del usuario.
- Los modos DISPONIBLE/NO DISPONIBLE se gestionarán mediante comandos “DoNotDisturb”

16.2.3 CÓMO CONFIGURAR EL SERVIDOR AVAYA IP OFFICE

Este apartado describe los procedimientos para configurar *Avaya IPOFFICE* para las siguientes áreas:

17. Cargar las licencias IPOFFICE IP Office CTI Link Pro en Avaya IP Office Manager PC
18. Configurar las extensiones utilizadas

19. Configurar los hunt-group utilizados
20. Configurar TAPI Wave Ports

Para instrucciones detalladas consulte el manual de AVAYA IPOFFICE.

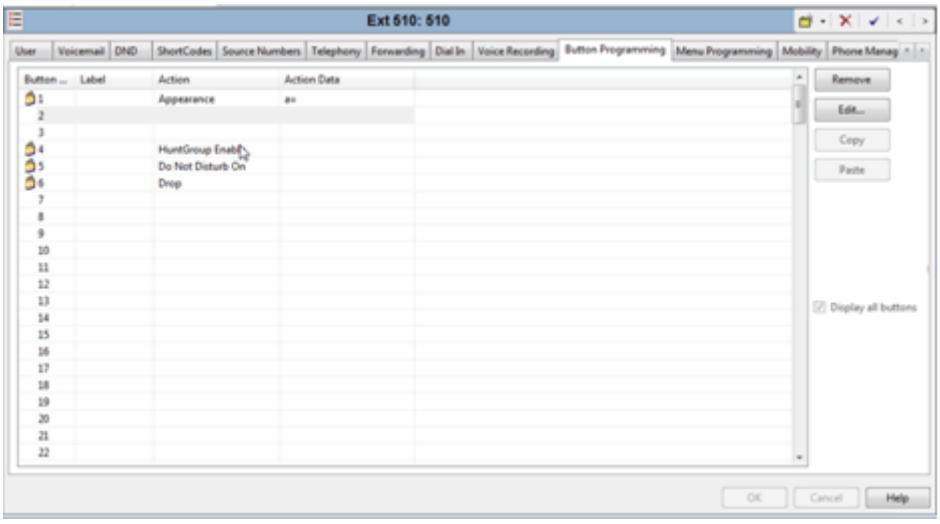
16.2.3.1 CARGAR LAS LICENCIAS IP OFFICE CTI LINK PRO EN IP OFFICE MANAGER PC.

1- Ir a Start > Programs > IP Office > Manager y ejecute la aplicación “Avaya IP Office Manager”
2- Ir a File > Open Configuration para mostrar el dialogo de selección de IP Office.
3- Seleccione el sistema IP Office e identifíquese con el usuario y contraseñas adecuados.
4- En el árbol de configuración, pulse el botón secundario del ratón sobre “License” y seleccione “New”
5- Entre el código del “CTI Link Pro license” en el campo “License key” y pulse ok
6- File > Save configuration

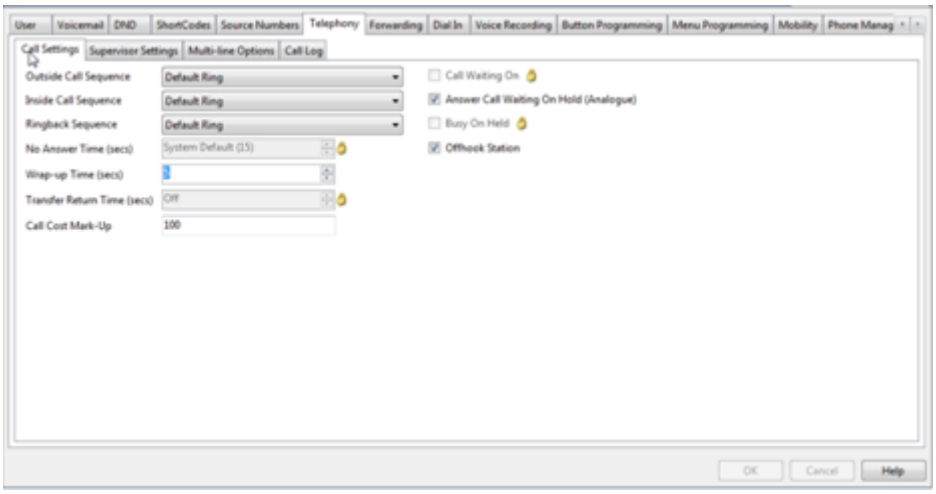
16.2.3.2 CONFIGURAR LAS EXTENSIONES UTILIZADAS

Administre las extensiones IPOFFICE que vayan a utilizase para los agentes. Para cada extensión, verifique:

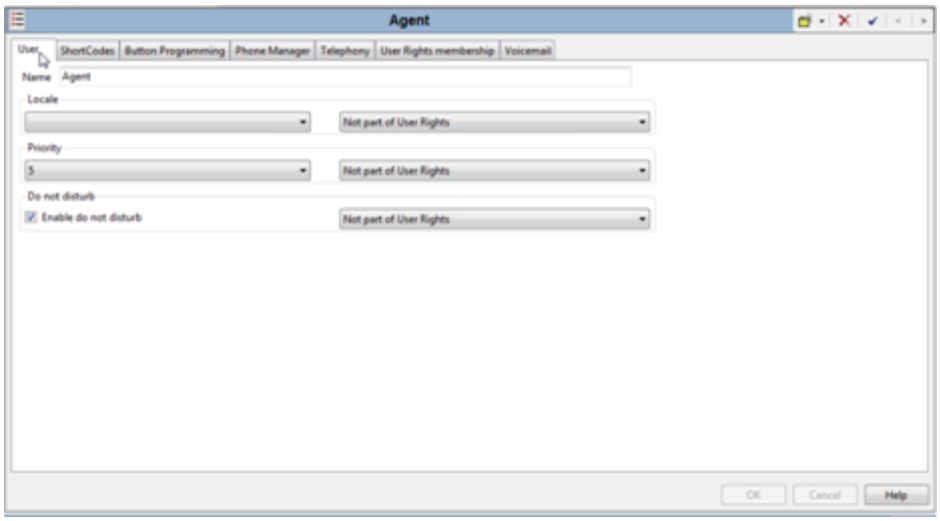
7- En el árbol de configuración de IP Office Manager PC | User, seleccione la extensión a configurar.
8- Click en el TAB “Button Programming” y configure para que la extensión solamente disponga de una única *appearance.* El uso de extensiones con múltiples *apperances* no está soportado.



9- Click en el TAB “Telephony”, y especifique Wrap-up Time (secs)=5, y seleccione la opción “Offhook Station”



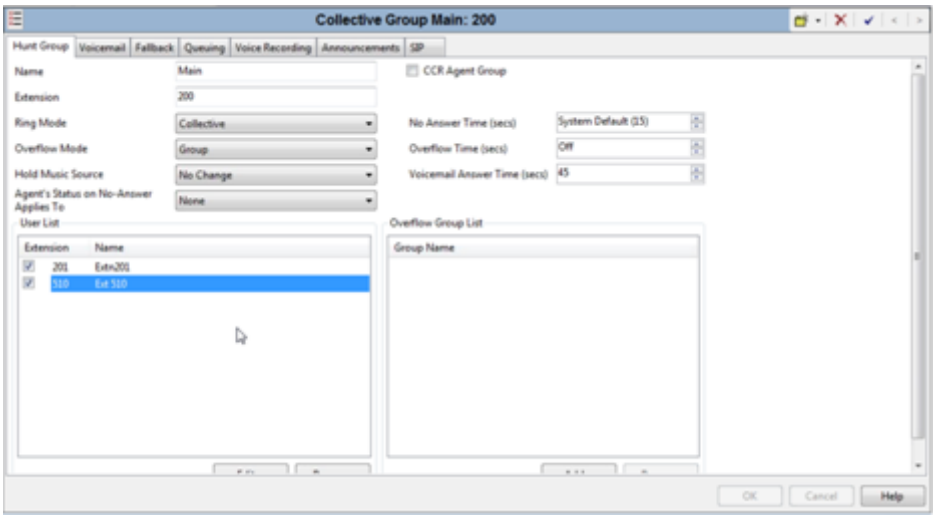
10- En el árbol de configuración seleccione “User Rights”, y el perfil asociado a los usuarios. P. ej: “User Rights | Agent”. En el TAB “User” seleccione la opción “Enable do not disturb”



16.2.3.3 CONFIGURAR LOS HUNT-GROUP UTILIZADOS

Administre los Hunt-Group IPOFFICE que vayan a utilizase para tratar las llamadas. Consulte el manual de AVAYA IPOFFICE.

11- En el árbol de configuración de IP Office Manager PC | HuntGroup, crear un nuevo Hunt Group. En el TAB “Hunt Group”, editar la “User list” para añadir los usuarios/extensiones del grupo, con el *checkmark* marcado.

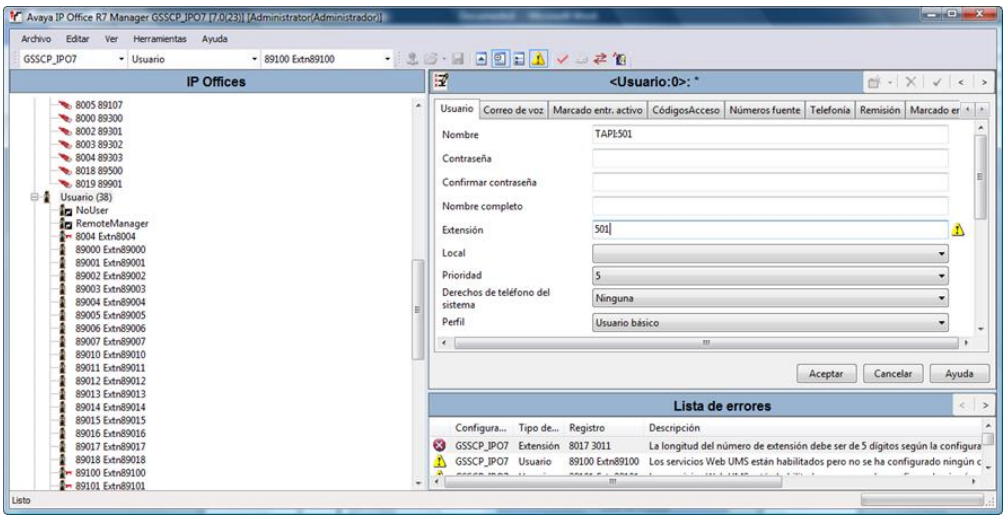


16.2.3.4 CONFIGURAR TAPI WAVE PORTS

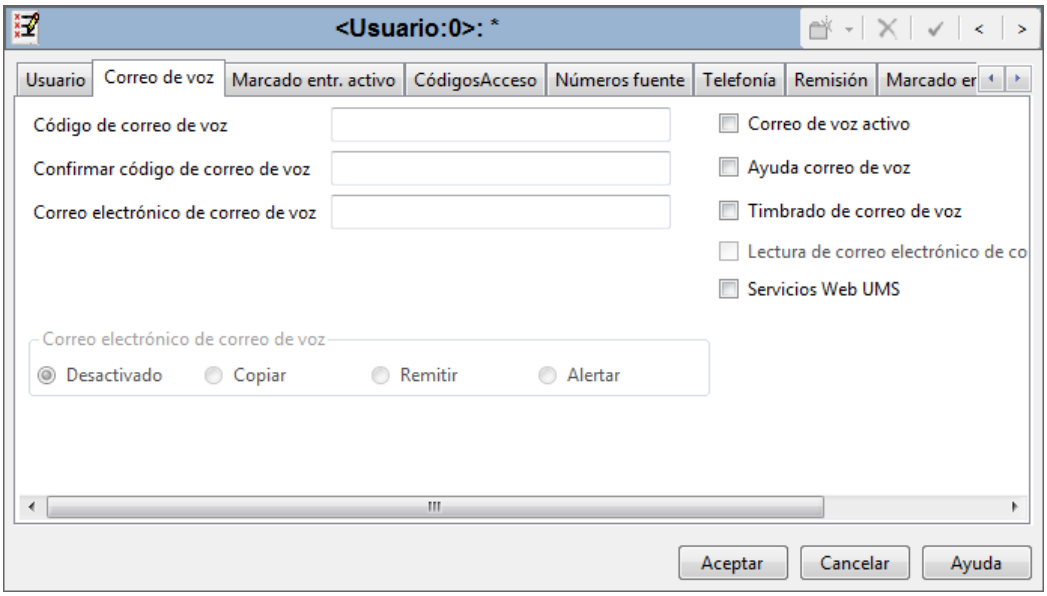
El módulo marcador predictivo/progresivo de Evolution utilizará "TAPI Wave port users" para iniciar las llamadas outbound. Deberán configurarse un número suficiente de Wave Ports en un rango consecutivo.

Para añadir un "wave port"

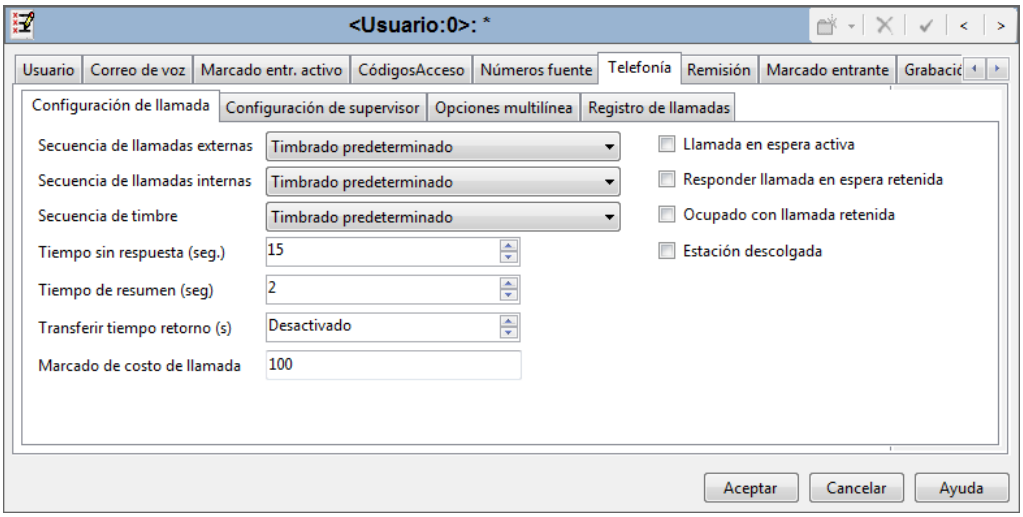
12- En el árbol de configuración de IP Office Manager PC, pulse con el botón secundario del ratón sobre "User" y seleccione "New".
13- Click en el TAB "User" y configure los campos
    a. Name: Entre "TAPI:x", donde "x" es un número que identifica el wave port concreto, p.ex: "TAPI:500"
    b. Extension: entre un número de extensión válido para la nueva extensión. El número de extensión no debería coincidir con ninguno preexistente. P.ej: "500"



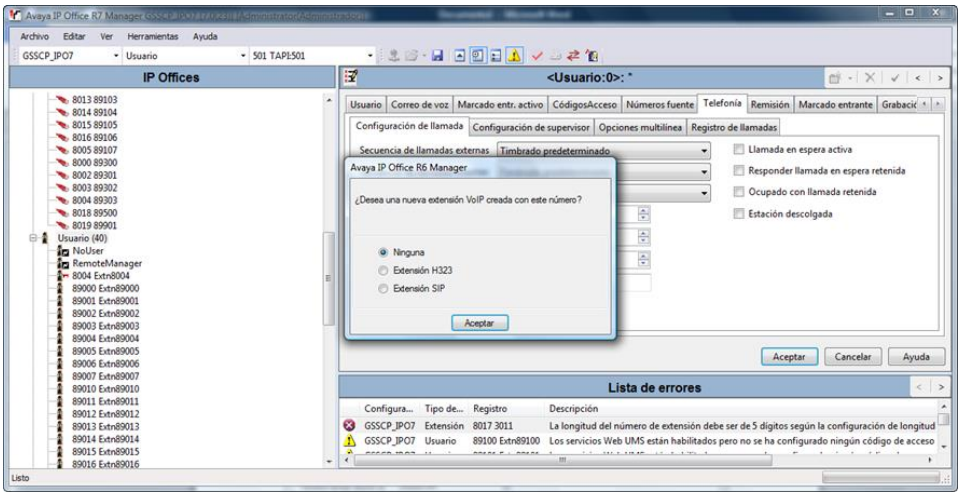
14- Click en el TAB "voicemail", y desmarque "Voicemail on"



15- Click en el TAB “telephony”, y desmarque “Answer call waiting on hold (analog)”



16- Una vez creado el usuario, se le solicita si desea crear una extensión VoIP con el número de extensión creado. Indicaremos que no deseamos crear ningún tipo de extensión.



17- Repita este proceso para cada wave port requerido.

Los puertos “Wave Ports” de IPOffice se comparten en el mismo pool de “data channels” usados para los puertos de “voicemail”.

El número máximo de canales de datos disponibles para llamadas simultáneas de voicemail y TAPI WAV calls depende del tipo de IP Office Control Unit:

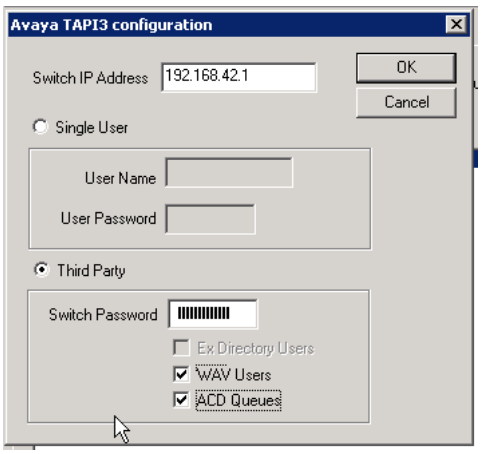
Control Unit	Data Channels	Channels usable for Voicemail/TAPI WAV
Small Office Edition	–	10
IP403	18	10
IP406 V1	24	20
IP406 V2	50	20
IP412	108	30
IP500	48	40
IP500 V2	48	40

16.2.4 CÓMO INSTALAR EL CLIENTE IPOFFICE TAPI3 (TAPI SERVICE PROVIDER)

Instale el componente “IPOFFICE TAPI3 (TAPI Service Provider)” en el servidor Evolution, de acuerdo con las instrucciones del fabricante (AVAYA).

Nota importante: No instalar la opción “Wave driver”.

18- Ejecute la instalación del “IP Office User Suite”
19- Seleccione el componente “TAPI”, pulse “siguiente”, y una vez completado el *wizard* de instalación, pulse “Finish”
20- Una vez instalado IPOFFICE TAPI3 ir al “Panel de Control”, “Phone & Modem Options”, TAB “Advanced”, seleccionar AVAYA TAPI3 y pulse “Configuration”. Entre los valores requeridos:
    - Switch IP address (ej: 192.168.42.1)
    - Seleccionar la opción “Third Party”
    - Switch password
    - Seleccionar las opciones “WAV Users”, “ACD Queues”

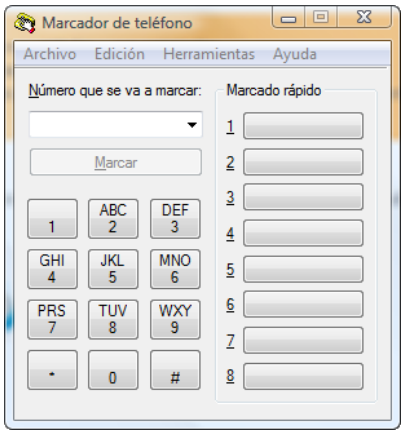


21- Para que cambios TAPI tengan efecto debe reiniciar el servidor.

16.2.5 CÓMO COMPROBAR EL CORRECTO FUNCIONAMIENTO DE IPOFFICE TAPI SERVICE PROVIDER

Comprueba el correcto funcionamiento del conjunto AVAYA IP OFFICE/AVAYA TAPI3 con la utilidad Microsoft Dialer.

Esta aplicación permite realizar una llamada entre dos extensiones, a través de TAPI.

Cómo comprobar el correcto funcionamiento del conjunto AVAYA IP OFFICE/AVAYA TAPI3	
1	Desde el menú de inicio Windows, opción “ejecutar”, ejecuta la utilidad “dialer.exe” 
2	Aparecerá el diálogo “Conectar usando”. En caso contrario acceder a él mediante el menú “Herramientas | conectar usando” y seleccionar la línea correspondiente a una extensión que hayamos configurado en IPOffice, p.ej: “IP Office Phone: 510"
3	En el “dialpad” telefónico marca una extensión de destino, p. ejemplo: 401
4	Cuando pulses “marcar” debería establecerse una llamada desde la extensión de origen (510), y con destino a la extensión indicada (401).

16.2.6 ¿QUÉ HACER SI NO APARECEN LAS EXTENSIONES RECIENTEMENTE CONFIGURADAS?

Si en el diálogo de “Conectar usando” de MS dialer no aparecen las extensiones de Avaya IP Office puede ser debido a un problema de configuración del IPOFFICE TAPI3 SERVICE PROVIDER. Revise los apartados anteriores.

Tenga en cuenta que si ha configurado una nueva extensión en el Administrador de Avaya IP Office, esta nueva extensión **no aparecerá hasta que no reinicie el servidor** donde está instalado IPOFFICE TAPI3 SERVICE PROVIDER.

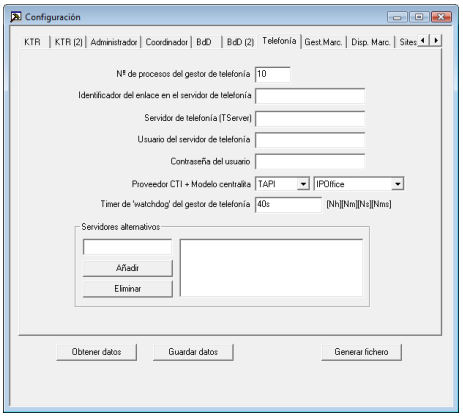
16.2.7 CÓMO CONFIGURAR EL ENLACE EVOLUTION AL SERVIDOR IPOFFICE AVAYA

A través de Evoadmin.exe, diálogo de “Configuración”, TAB “Telefonía”, edite los siguientes **parámetros de telefonía:**

Parámetro	Valor	Ejemplos
Identificador del enlace en el servidor de telefonía	(vacío)	
Servidor de telefonía Tserver	(vacío)	
Usuario y contraseña del servidor de telefonía	(vacío)	
Proveedor CTI + Modelo centralita	TAPI / IPOFFICE	TAPI / IPOFFICE

Configuración de telefonía en evoadmin

Ejemplo de configuración en Evoadmin



16.2.8 CÓMO CONFIGURAR EL MÓDULO ICR DIALER DAEMON (EVODIALERSERVER)

Configuración del Servidor de Marcación con AVAYA IPOFFICE usando "WAV PORTS"	
1	Iniciar c:\ICR\Evolution\Server\DialerParam.exe
2	Indicar la Máquina donde está instalado el Servidor de Marcación y pulsar Obtener Datos. Ej: "Maquina de Dialer": "." (un punto, indicando local)
3	En la pestaña DialerGlobal: > **Module** escribir el número Module=62 que es el correspondiente al tipo TAPIIPOFFICE. >**MainLinkID, MainServerID, MainLogin/MainPwd** dejar vacíos
4	En la pestaña CTIDIALER: Desmarcar **UseSlaveThal** > UseSlaveThal=NO
5	Y pulsamos Guardar Datos.

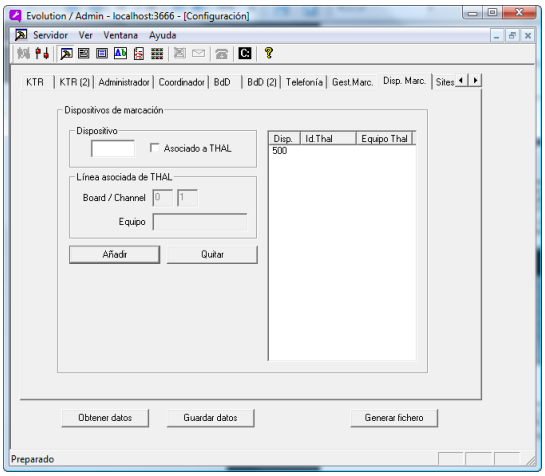
16.2.9 CÓMO ADMINISTRAR LOS DISPOSITIVOS DE MARCACIÓN EN EVOADMIN

Deberemos administrar los dispositivos de marcación en EvoAdmin, vinculándolos a los “wave port” definidos anteriormente en IP Office

Configuración de Dispositivos de Marcación en evoadmin

1 Ejecute evoadmin.exe, indique el *password* para operaciones restringidas, acceda al diálogo de “Configuración”, TAB “Disp. Marcador” y edite la lista de dispositivos de marcación para que corresponda con los WAV PORTS administrados anteriormente en IP Office.

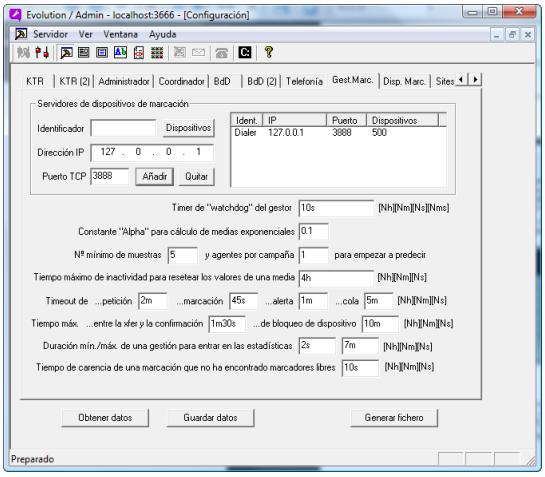
Pulse Guardar Datos.



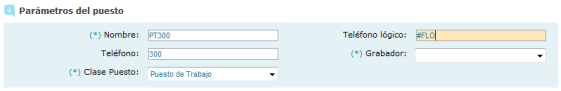
2 En el TAB “Gest. Marc.” pase a “off-line” el marcador seleccionando el identificador del “servidor de dispositivos de marcación” y pulsando el botón “Quitar”.

Pulse “Dispositivos”, edite la lista de dispositivos añadiéndole todos los dispositivos correspondientes a wave ports. Una vez editados pulse “Añadir” para pasar a “on-line”.

Pulse Guardar Datos.



16.2.10 CONFIGURACIONES DE EVOLUTION MANAGER

Configuración Manager		
1	Administración | Puestos	Informe el número de la extensión en el parámetro “teléfono” En el campo “teléfono lógico” escriba “#FLO” para indicar que se desea modo “flotante” (hot desking user) Ej: teléfono: 300, teléfono lógico=#FLO 
2	Administración | Usuarios	Informe en los parámetros de ACD el “login ACD” y “password ACD” administrados en AVAYA IPO. Cuando el agente Evolution se conecte, se utilizarán estos parámetros para efectuar el login AVAYA IPO mediante el envío de un secuencia correspondiente a USER-LOGIN, p.ej: “*35*123*456#”, donde 123 y 456 son el “login ACD” y “password ACD” Ej: Login ACD: 50001
3	Administración | Campañas	En la sección “Routing” seleccione la opción “switch-based” Evolution determina que las llamadas *inbound* pertenecen a una campaña cuando el `calleddevice` de la llamada coincide con el DN de una estrategia DNIS asociada a la campaña. Administre una o más estrategias de tipo DNIS, asociadas a la campaña. Normalmente en AvayaIPOFFICE el valor de DNIS debe coincidir con el número de HUNTGROUP que entrega las llamadas *inbound*.

En la sección “Routing” administre una o más estrategias de tipo de encaminamiento ‘DNIS’, y asígnela a la campaña.

Ej: Estrategia de encaminamiento tipo DNIS con DN: 100 y asociada a la campaña “atención al cliente”

En la administración de campaña informe el parámetro “Disp. De control” con el HUNTGROUP que deberá entregar las llamadas *outbound* a los agentes.

Si la campaña no usa marcación progresiva o predictiva puede dejar este campo vacío.

Ej: Disp. De control: 30001

16.2.11 LIMITACIONES CONOCIDAS DE EVOLUTION CON AVAYA IP OFFICE

1	En algunas situaciones el componente AVAYA TAPI3 Tapi Service Provider puede dejar de responder para determinadas extensiones.	Se resuelve cerrando el monitor TAPI de la extensión afectada. Un agente lo puede hacer cerrando/abriendo la sesión en la aplicación Evolution/agente.
2	Problemas con transferencias sucesivas de una llamada.	En determinadas situaciones el AVAYA TAPI3 TSP envía eventos incorrectos cuando una llamada que es retransferida sucesivamente y alcanza de nuevo una extensión anterior.

3	Si un agente recibe una una transferencia supervisada a través de ACD, no llega un evento transferred.	Como resultado el UI de iagent no se refresca y sigue mostrando el ANI de la extensión que ha provocado la llamada.
4	Si el usuario recibe una llamada INBOUND y pulsa el botón de COLGAR mientras la llamada está timbrando se le muestra un aviso que indica que no se puede colgar una llamada que está ALERTANDO.	Solamente pueden colgarse llamadas que están en estado “establecida”.
5	Si se llama a una extensión inexistente (Ej: llamada al 66666), se genera un señal audible de ‘numero no existe’ pero al pulsar el botón COLGAR de iagent no se cuelga la llamada.	La llamada se podrá colgar desde la extensión teléfono IPOffice

16.3 AVAYA CS1000 & CC7

NOTA: AVAYA CS1000 anteriormente se denominaba NORTEL CS1000

Recomendado: CTConnect 7.5

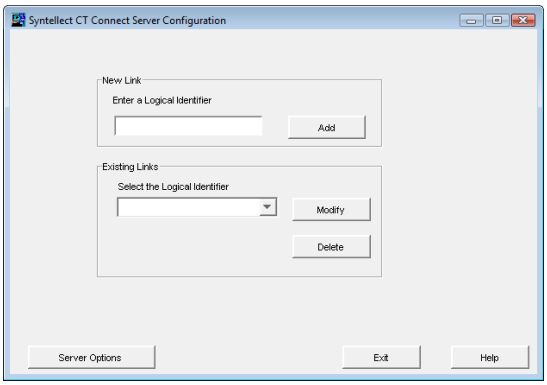
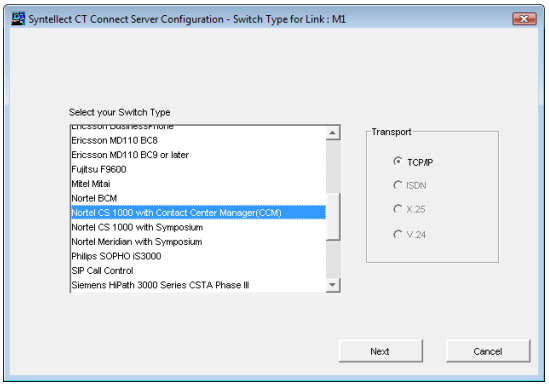
Evolution soporta los siguientes tipos de campaña con Avaya CS1000 y CC7:

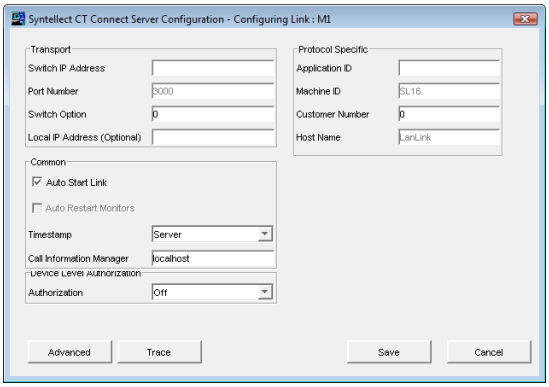
- Inbound switch based routing
- Outbound vp
- Outbound predictivo/progresivo

16.3.1 CÓMO CONFIGURAR EL SERVIDOR CTCONNECT SERVER

Instale el componente “Syntellect CTConnect server 7.5” de acuerdo con las instrucciones del fabricante (Syntellect). Este software puede instalarse en el mismo servidor que Evolution o en un servidor independiente. Tenga en consideración los requerimientos específicos de “Syntellect CTConnect server 7.5”.

Para configurar un enlace a AVAYA CS1000 (NORTEL CS1000)

1	Ejecutar la aplicación “Menú de Inicio | Syntellect CT Connect | Configuration Program” Crear un LINK, especificando un LOGICAL IDENTIFIER adecuado. P.ej: “CC7”	
2	Seleccionar el switch Type “Nortel CS 1000 with Contact Center Manager(CCM)”	

3	Configurar los parámetros que adecuados para el link administrado en CC7. Establezca el “Switch IP Address” correspondiente al servidor AVAYA CC7 (NORTEL CC7)	
4	Si es necesario, reiniciar el servidor, comprobar que el servicio Syntellect CT Connect está en iniciado y en modo modo inicio automático	
5	Podemos comprobar el nuevo link: 1- Aplicación “Menú de Inicio | Syntellect CT Connect | Control Program” 2- Informar el parametro CurrentServer y botón [REFRESH] debe mostrar el Logical Identifier, con el correspondiente Link State (UP)	

16.3.2 CÓMO INSTALAR EL CLIENTE SYNTELLECT CT CONNECT CLIENT

Instale el componente “Syntellect CT Connect client” en el servidor Evolution, de acuerdo con las instrucciones del fabricante (Syntellect).

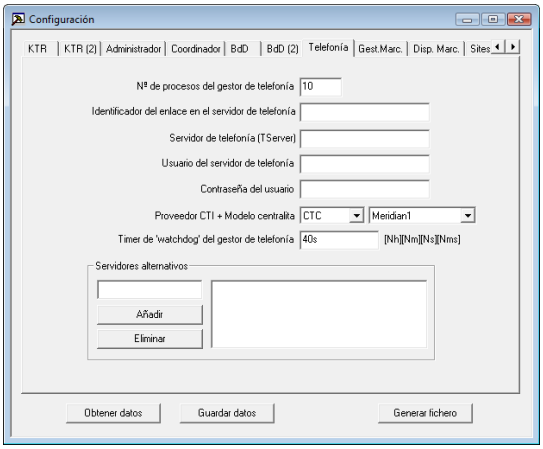
16.3.3 CÓMO CONFIGURAR EL ENLACE EVOLUTION AL SERVIDOR NORTEL CC7

A través de Evoadmin.exe se deberán configurar los siguientes **parámetros de telefonía:**

Parametro	Valor	Ejemplos
Identificador del enlace en el servidor de telefonía	Corresponde al “LOGICAL ID” configurado en CTConnect server	“M1” o CC7”
Servidor de telefonía Tserver	Dirección IP del servidor CTConnect	192.168.1.105 o localhost
Usuario y contraseña del servidor de telefonía	(vacío)	
Proveedor CTI + Modelo centralita	CTC / Meridian1	CTC / Meridian1

Configuración de telefonía en evoadmin

Ejemplo de configuración en Evoadmin



16.3.4 CÓMO CONFIGURAR EL MÓDULO ICR DIALER DAEMON (EVODIALERSERVER)

Configuración del Servidor de Marcación con AVAYA CC7 (NORTEL) usando "Phantom"

El termino **Phantom** se refiere a un dispositivo con una extensión pero sin un terminal físico asociado, este dispositivo es específico deAVAYA CS1000 (NORTEL) y permite la Marcación automática CTI.

1 Iniciar c:\ICR\Evolution\Server\DialerParam.exe

2 Indicar la Máquina donde está instalado el Servidor de Marcación y pulsar Obtener Datos.

Ej: "Maquina de Dialer": "." (un punto, indicando local)

3 En la pestaña DialerGlobal:

> **Module** escribir el número 68 que es el correspondiente al tipo CtcMeridian1Phantom.

>**MainLinkID** escribir el mismo valor que hayamos indicado en el parámetro "Identificador del enlace en el servidor de telefonía" en evoadmin. P.ej: "CC7"

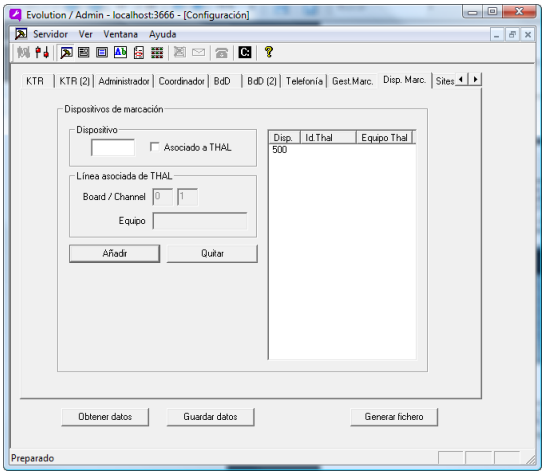
	>**MainServerID** nombre del servidor de telefonía. Escribir el mismo valor que hayamos indicado en el parámetro “Servidor de telefonía Tserver” en evoadmin. P.ej: “192.168.1.110” >**MainLogin/MainPwd** usuario/contraseña. Dejar vacios.
4	Y pulsamos Guardar Datos.

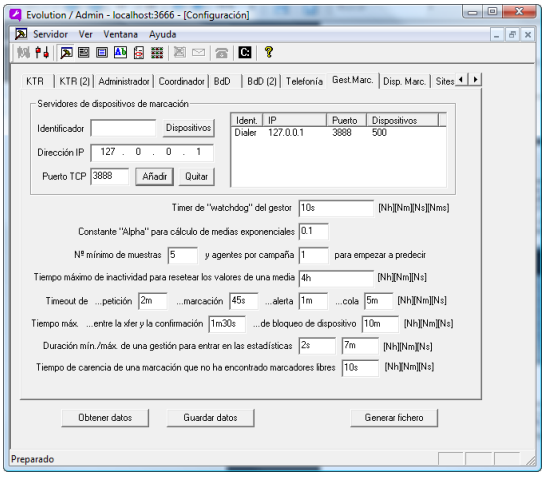
16.3.5 CÓMO ADMINISTRAR LOS DISPOSITIVOS DE MARCACIÓN EN EVOADMIN

En el caso de utilizar PHANTOMS AVAYA CS1000, los dispositivos de marcación Evolution deben corresponder con dispostivos “phantom” administrados en CS-1000.

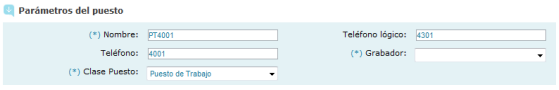
Debe administrar un número suficiente y adecuado de dispositivos de marcación en Evoadmin, para soportar los procesos de marcacion.

Configuración de Dispositivos de Marcación en evoadmin	
1	Ejecute evoadmin.exe, indique el *password* para operaciones restringidas, acceda al diálogo de “Configuración”, TAB “Disp. Marcador” y edite la lista de dispositivos de marcación. Pulse Guardar Datos.



2	En el TAB “Gest. Marc.” pase a “off-line” el marcador seleccionando el identificador del “servidor de dispositivos de marcación” y pulsando el botón “Quitar”. Pulse “Dispositivos”, edite la lista de dispositivos añadiéndole todos los dispositivos correspondientes a wave ports. Una vez editados pulse “Añadir” para pasar a “on-line”. Pulse Guardar Datos.	

16.3.6 CONFIGURACIONES DE EVOLUTION MANAGER

	Configuración Manager	
1	Administración | Puestos	Informe el número extensión (DN) de la extensión en el parámetro “teléfono” Informe el número de Position-ID (POSID) de la extensión en el parámetro “teléfono lógico” Ej: teléfono: 4001, teléfono lógico=4301 
2	Administración | Usuarios	Informe en los parámetros de ACD el “login ACD” y “password ACD” administrados en AVAYA. Cuando el agente Evolution se conecte, se utilizarán estos parámetros para efectuar el login CC7. Ej: Login ACD: 50001

3	Administración | Campañas	En la sección “Routing” seleccione la opción “switch-based” Evolution determina que las llamadas inbound pertenecen a una campaña cuando el calleddevice de la llamada coincide con el DN de una estrategia DNIS asociada a la campaña. Administre una o más estrategias de tipo DNIS, asociadas a la campaña. Normalmente en Avaya CS1000 el valor de DNIS debe coincidir con el número de CDN que entrega las llamadas *inbound*. En la sección “Routing” administre una o más estrategias de tipo de encaminamiento ‘DNIS’, y asígnela a la campaña. Ej: Estrategia de encaminamiento tipo DNIS con DN: 100 y asociada a la campaña “atención al cliente” Informe el parámetro “Disp. De control” con el CDN que deberá generar las llamadas predictivas/progresivas. Si la campaña no usa marcación progresiva o predictiva puede dejar esta campo vacío Ej: Disp. De control: 30001

16.4 NORTEL MERIDIAN-1 & SYMPOSIUM 5/6

Recomendado: CTConnect 7.5

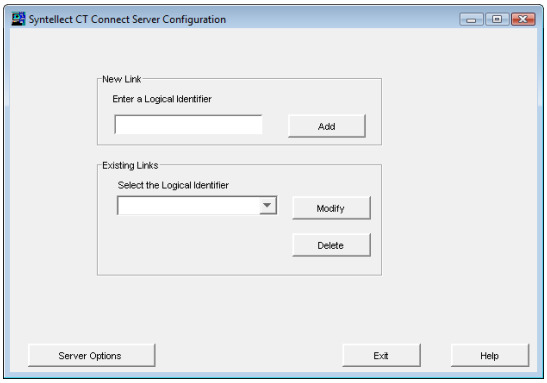
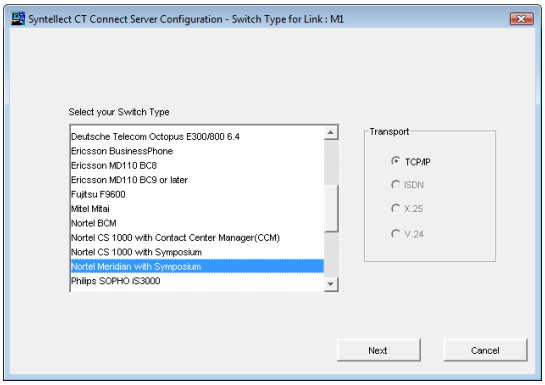
Evolution soporta los siguientes tipos de campaña con Nortel Meridian-1 y Symposium:

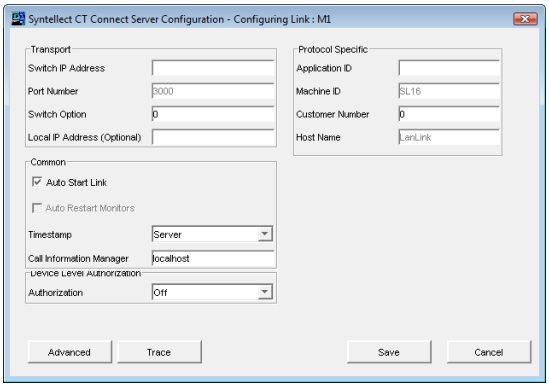
- Inbound switch based routing
- Outbound vp
- Outbound predictivo/progresivo

16.4.1 CÓMO CONFIGURAR EL SERVIDOR CTCONNECT SERVER

Instale el componente “Syntellect CTConnect server 7.5” de acuerdo con las instrucciones del fabricante (Syntellect). Este software puede instalarse en el mismo servidor que Evolution o en un servidor independiente. Tenga en consideración los requerimientos específicos de “Syntellect CTConnect server 7.5”.

Para configurar un enlace a NORTEL SYMPOSIUM

1	Ejecutar la aplicación “Menú de Inicio | Syntellect CT Connect | Configuration Program” Crear un LINK, especificando un LOGICAL IDENTIFIER adecuado. P.ej: “M1”	
2	Seleccionar el switch Type “Nortel Meridian with Symposium”	

3	Configurar los parámetros adecuados para el link administrado en Symposium. Establezca el “Switch IP Address” correspondiente al servidor NORTEL SYMPOSIUM	
4	Si es necesario, reiniciar el servidor, comprobar que el servicio Syntellect CT Connect está en iniciado y en modo modo inicio automatico	
3	Podemos comprobar el nuevo link: ▪ Aplicación “Menú de Inicio | Syntellect CT Connect | Control Program” ▪ Informar el parametro CurrentServer y botón [REFRESH] debe mostrar el Logical Identifier, con el correspondiente Link State (UP)	

16.4.2 CÓMO INSTALAR EL CLIENTE SYNTELLECT CT CONNECT CLIENT

Instale el componente “Syntellect CT Connect client” en el servidor Evolution, de acuerdo con las instrucciones del fabricante (Syntellect).

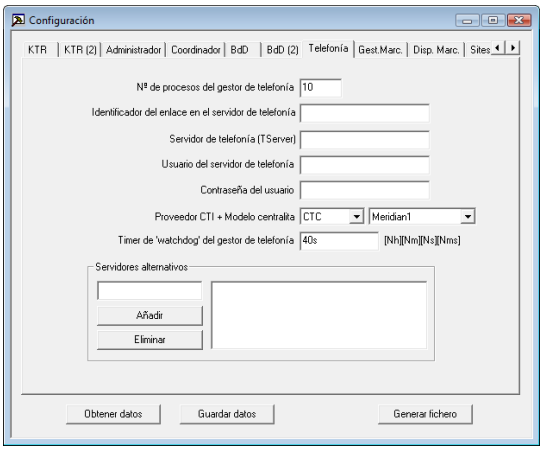
16.4.3 CÓMO CONFIGURAR EL ENLACE EVOLUTION AL SERVISOR SYMPOSIUM

A través de Evoadmin.exe se deberán configurar los siguientes **parámetros de telefonía:**

Parametro	Valor	Ejemplos
Identificador del enlace en el servidor de telefonía	Corresponde al "LOGICAL ID" configurado en CTConnect server	"M1"
Servidor de telefonía Tserver	Dirección IP del servidor CTConnect	192.168.1.105 o localhost
Usuario y contraseña del servidor de telefonía	(vacío)	
Proveedor CTI + Modelo centralita	CTC / Meridian1	CTC / Meridian1

Configuración de telefonía en evoadmin

Ejemplo de configuración en Evoadmin



16.4.4 CÓMO CONFIGURAR EL MÓDULO ICR DIALER DAEMON (EVODIALERSERVER)

Configuración del Servidor de Marcación con NORTEL CC7 usando "Phantom"

El termino **Phantom** se refiere a un dispositivo con una extensión pero sin un terminal físico asociado, este dispositivo es específico de la Nortel Meridian-1 y permite la Marcación automática CTI.

1	Iniciar c:\ICR\Evolution\Server\DialerParam.exe
2	Indicar la Máquina donde está instalado el Servidor de Marcación y pulsar Obtener Datos. Ej: "Maquina de Dialer": "." (un punto, indicando local)
3	En la pestaña DialerGlobal: > **Module** escribir el número 68 que es el correspondiente al tipo CtcMeridian1Phantom. >**MainLinkID** escribir el mismo valor que hayamos indicado en el parámetro "Identificador del enlace en el servidor de telefonía" en evoadmin. P.ej: "M1" >**MainServerID** nombre del servidor de telefonía. Escribir el mismo valor que hayamos indicado en el parámetro "Servidor de telefonía Tserver" en evoadmin. P.ej: "192.168.1.110" >**MainLogin/MainPwd** usuario/contraseña. Dejar vacios.
4	Y pulsamos Guardar Datos.

16.4.5 CÓMO ADMINISTRAR LOS DISPOSITIVOS DE MARCACIÓN EN EVOADMIN

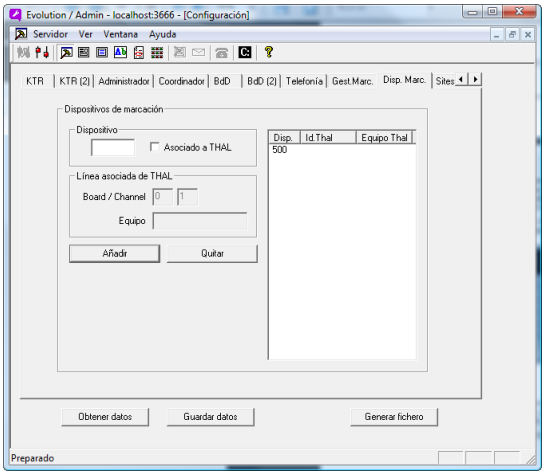
En el caso de utilizar PHANTOMS MERIDIAN-1, los dispositivos de marcación Evolution deben corresponder con dispostivos "phantom" administrados en M1.

Debe administrar un número suficiente y adecuado de dispositivos de marcación en Evoadmin, para soportar los procesos de marcacion.

Configuración de Dispositivos de Marcación en evoadmin

1 Ejecute evoadmin.exe, indique el *password* para operaciones restringidas, acceda al diálogo de "Configuración", TAB "Disp. Marcador" y edite la lista de dispositivos de marcación.

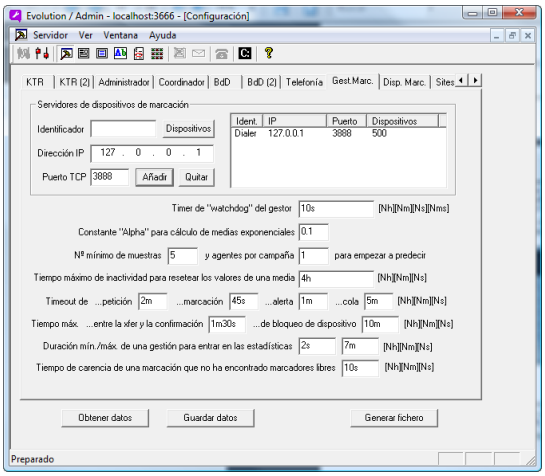
Pulse Guardar Datos.



2 En el TAB "Gest. Marc." pase a "off-line" el marcador seleccionando el identificador del "servidor de dispositivos de marcación" y pulsando el botón "Quitar".

Pulse "Dispositivos", edite la lista de dispositivos añadiéndole todos los dispositivos correspondientes a wave ports. Una vez editados pulse "Añadir" para pasar a "on-line".

Pulse Guardar Datos.


Evolution / Admin - localhost:3666 - [Configuración]
Servidor Ver Ventana Ayuda
KTR KTR (2) Administrador Coordinador BdD BdD (2) Telefonía Gest.Marc. Disp. Marc. Sites
Servidores de dispositivos de marcación
Identificador
Dispositivos
Dirección IP 127 . 0 . 0 . 1
Puerto TCP 3888
Añadir
Quitar
Ident. IP Puerto Dispositivos
Dialer 127.0.0.1 3888 500
Timer de "watchdog" del gestor 10s [Nh][Nm][Ns][Nms]
Constante "Alpha" para cálculo de medias exponenciales 0.1
Nº mínimo de muestras 5 y agentes por campaña 1 para empezar a predecir
Tiempo máximo de inactividad para resetear los valores de una media 4h [Nh][Nm][Ns]
Timeout de ...petición 2m ...marcación 45s ...alerta 1m ...cola 5m [Nh][Nm][Ns]
Tiempo máx. ...entre la xfer y la confirmación 1m30s ...de bloqueo de dispositivo 10m [Nh][Nm][Ns]
Duración mín./máx. de una gestión para entrar en las estadísticas 2s 7m [Nh][Nm][Ns]
Tiempo de carencia de una marcación que no ha encontrado marcadores libres 10s [Nh][Nm][Ns]
Obtener datos
Guardar datos
Generar fichero
Preparado

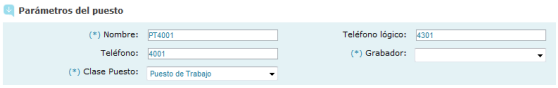
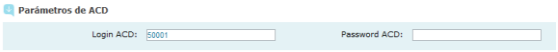
16.4.6 CONFIGURACIONES DE EVOLUTION MANAGER

Configuración Manager

1 Administración | Puestos

Informe el número extensión (DN) de la extensión en el parámetro "teléfono"

Informe el número de Position-ID (POSID) de la

		extensión (DN) en el parámetro “teléfono lógico” Ej: teléfono: 4001, teléfono lógico=4301 
2	Administración | Usuarios	Informe en los parámetros de ACD el “login ACD” y “password ACD” administrados en AVAYA. Cuando el agente Evolution se conecte, se utilizarán estos parámetros para efectuar el login CC7. Ej: Login ACD: 50001 
3	Administración | Campañas	En la sección “Routing” seleccione la opción “switch-based” Evolution determina que las llamadas inbound pertenecen a una campaña cuando el calleddevice de la llamada coincide con el DN de una estrategia DNIS asociada a la campaña. Administre una o más estrategias de tipo DNIS, asociadas a la campaña. Normalmente en Nortel Meridian-1 el valor de DNIS debe coincidir con el número de CDN que entrega las llamadas inbound. En la sección “Routing” administre una o más estrategias de tipo de encaminamiento ‘DNIS’, y asígnela a la campaña. Ej: Estrategia de encaminamiento tipo DNIS con DN: 100 y asociada a la campaña “atención al cliente” Informe el parámetro “Disp. De control” con el CDN que deberá generar las llamadas predictivas/progresivas. Si la campaña no usa

	marcación progresiva o predictiva puede dejar esta campo vacío Ej: Disp. De control: 30001

16.5 CISCO COMMUNICATIONS MANAGER CM/UCM

Recomendado con TAPI CISCO.

Evolution soporta los siguientes tipos de campaña con CISCO CM:

- Inbound DBR
- Outbound VP
- Outbound predictivo/progresivo DBR

Para los modos Inbound DBR y Outbound predictivo/progresivo DBR, Evolution hace uso de un dispositivo 'CTI Route Point' para cada estrategia DBR.

Para el modo Outbound predictivo/progresivo DBR, Evolution hace uso de un 'pool' de dispositivos 'CTI Port', como dispositivos de marcación.

16.5.1 CONFIGURACIÓN CERTIFICADA

La siguiente es la lista de equipos y software que se utilizó para la validación y certificación de Evolution en un entorno CISCO CM:

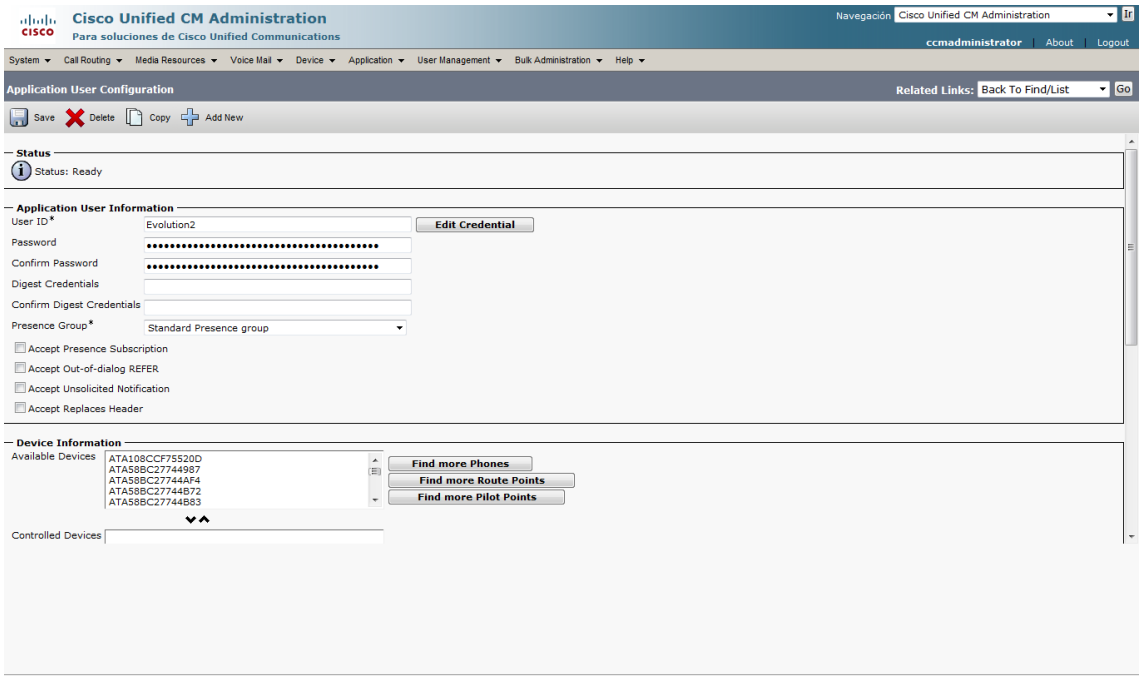
Equipamiento	Software
Cisco Unified Communications Manager	Release 7.1.3
IP softphone	CISCO IP Communicator v7.0.3.3
Cisco TSP for Windows32	Version 7.1(3.4)
Evolution 10	Windows W2003 Server R2 32 bits SQL server 2008 Express

16.5.2 CÓMO ADMINISTRAR UN USUARIO CISCO PARA EVOLUTION

Se debe configurar un usuario Cisco con privilegios adecuados para que EVOLUTION se comunique como cliente TAPI con el servidor CM.

Acceder a **Cisco Unified CM Administration → User Management → Application User** y seleccionar **Add New**, configurando los siguientes parámetros:

1. **User ID –** Este es el usuario que deberá ser utilizado por Evolution. Por ejemplo: "Evolution2"
2. **Password y Confirm Password:** Selecciona una contraseña
3. **Permissions Information, Add to User Group:** Añadir a todos los grupos **'**Standard CTI xxx**'.**
4. Finalmente pulse "**Save"**



16.5.3 CÓMO ASOCIAR LAS LÍNEAS DE LOS TELÉFONOS AL USUARIO EVOLUTION

Para que las líneas de los teléfonos (dispositivos tipo *phone*) puedan ser controladas por el servidor Evolution éstas deben asociarse a un usuario Cisco con privilegios adecuados. Para ello, acceda a **Cisco Unified CM Administration → User Management → Application User**:

1. Seleccione el usuario. P. ej: “Evolution2”
2. En la sección “Device Information” identifique las líneas correspondientes a los números que desea asociar y añádalas a la lista de “controlled devices”

Repita los anteriores pasos para cada teléfono que desee controlar en el call center Evolution.

16.5.4 CÓMO CONFIGURAR LOS DISPOSITIVOS CTI ROUTE POINT NECESARIOS

El módulo Evolution DBR hace uso de dispositivos Cisco CTI Route Point para encaminar las llamadas a las extensiones de los agentes. Cada estrategia DBR en Evolution requiere su correspondiente CTI Route Point.

Para crear dispositivos CTI Route Point, accede a **Cisco Unified CM Administration → Device → CTI Route Point**:

1. Administre un CTI Route Point existente o cree uno nuevo, pulsando ‘Add New’
2. Configure “Device Name”. Ej: “111”
3. Desde la sección “Association Information” cree una línea pulsando en el enlace “Line [1] – Add a new DN”.
4. En el formulario “Directory Number Configuration”.correspondiente al DN de la nueva línea que acaba de crear, administre el parámetro Directory Number. Ej: “Directory Number” = 111

Deberemos asignar los dispositivos CTI ROUTE POINT al usuario de aplicación que utilizará Evolution. Para ello, acceda a **Cisco Unified CM Administration → User Management → Application User**:

1. Seleccione el usuario. P. ej: “Evolution2”
2. En la sección “Device Information” identifique las líneas correspondientes a los números CTI Route Point que desea asociar y añádalas a la lista de “controlled devices”

Repita los anteriores pasos para cada CTI Route Point que desee controlar en el call center Evolution.

16.5.5 CÓMO ADMINISTRAR RUTAS DE LLAMADAS ENTRANTES EN CISCO CM

Debe administrar Cisco CM para que dirija las llamadas entrantes a los dispositivos CTI Route Point adecuados. Una forma de conseguirlo es utilizando “Translation Patterns”.

Acceda a **Cisco Unified CM Administration → Call Routing → Translation Pattern**:

1. Administre un “Translation Pattern” existente o cree uno nuevo, pulsando ‘Add New’
2. En la sección “Called Party Transformations”, configure “Called Party Transform Mask”. P. ej: “Called Party Transform Mask”=110
3. Guarde los cambios con “Save”

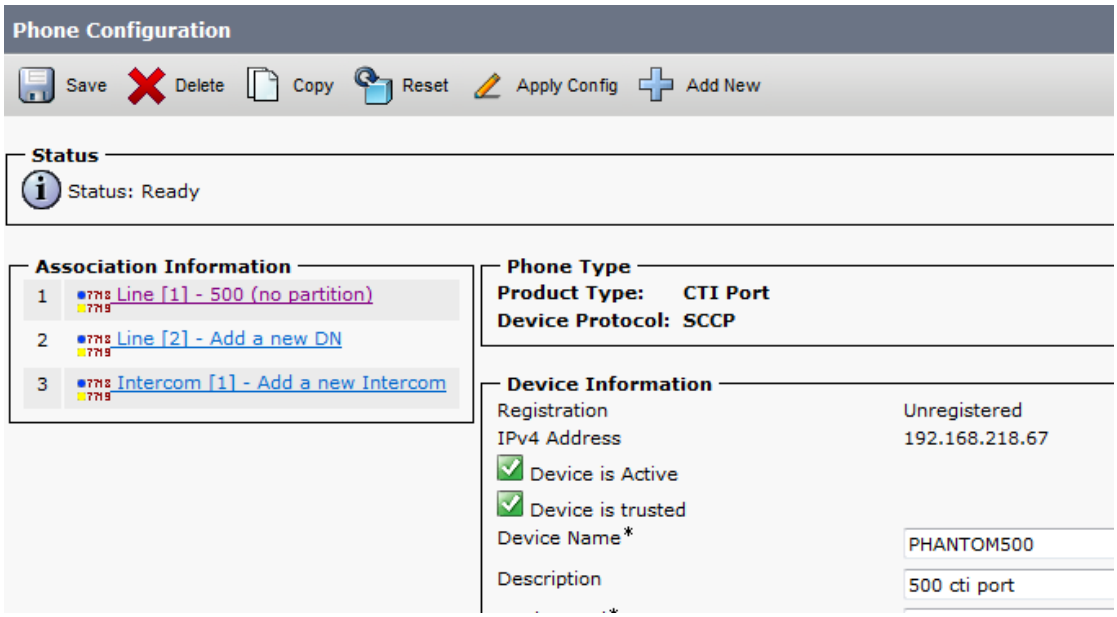
16.5.6 CÓMO CONFIGURAR LOS DISPOSITIVOS CTI PORTS NECESARIOS

El módulo Evolution Dialer hace uso de dispositivos de marcación para generar las llamadas de las campañas las campañas predictivo o progresivo. Por ello se requiere configurar un número suficiente de dispositivos.

En una arquitectura con Cisco CM estos dispositivos de marcación deberán corresponder a dispositivos de tipo Cisco CTI Port.

Para ello acceda a **Cisco Unified CM Administration → Device → Phone**:

1. Administre un dispositivo de tipo CTI Port existente o cree uno nuevo, pulsando ‘Add New’, Phone Type=CTI Port, Next
2. Configure Device Name. Ej: “PHANTOM500”
3. En la sección “Protocol Specific Information” configure “Device Security Profile”. Ej: “Cisco CTI Port – Standard SCCP Non-Secure Profile”
4. Desde la sección “Association Information” cree una línea pulsando en el enlace “Line [1] – Add a new DN”.



Deberemos asignar los dispositivos CTI PORT al usuario de aplicación que utilizará Evolution. Para ello, acceda a **Cisco Unified CM Administration → User Management → Application User**:

1. Seleccione el usuario. P. ej: "Evolution2"
2. En la sección "Device Information" identifique las líneas correspondientes a los números CTI Port que desea asociar y añádalas a la lista de "controlled devices"

Repita los anteriores pasos para cada cti-port que desee controlar en el call center Evolution.

Nota
Los dispositivos CISCO CTI PORT utilizan el códec G.711. Por ello deberán administrarse en una región que fuerce el uso de este tipo de códec. De lo contario, y si no puede negociarse un códec común en ambos extremos de la llamada. pueden producirse cortes en las llamadas de marcador.

16.5.7 CÓMO INSTALAR LOS COMPONENTES CISCOTSP Y CISCO WAVE DRIVER

Deben instalarse los componentes **CiscoTSP (Cisco Unified Communications Manager TSP)** y **Cisco Wave Driver** en el mismo servidor que ejecuta Evolution Server.

Puuede obtener el componente CiscoTSP descargándolo del propio portal de administración **Cisco Unified CM Administration.** Para ello acceda a **Cisco Unified CM Administration → Application → Plugins** y identifique y descargue el componente denominado "Cisco Telephony Service Provider", al que en adelante nos referiremos como CiscoTSP.

Instale este componente CiscoTSP (Cisco Unified Communications Manager TSP) en el servidor Evolution, siguiendo las instrucciones del fabricante. Una vez instalado deberá configurarlo, accediendo a los diálogos de configuración:

1. Panel de Control → Opciones de teléfono y módem → Opciones avanzadas, seleccionar CISCOTSPxxx.tsp y 'configurar'
2. En "User" especificar el User Name, Pssword y Verify Password correspondientes al usuario Evolution que previamente hayamos administrado en **Cisco Unified CM Administration**. Ej: "Evolution"
3. En "CTI Manager", especificar la dirección IP correspondiente al "CISCO CTI Manager". Ej: 192.168.218.10
4. En "Wave" asegurarse que "Enumerate only lines which support Automated Voice" **NO** esta seleccionado.
5. Guardar todos los cambios con "OK", y reiniciar el servidor.

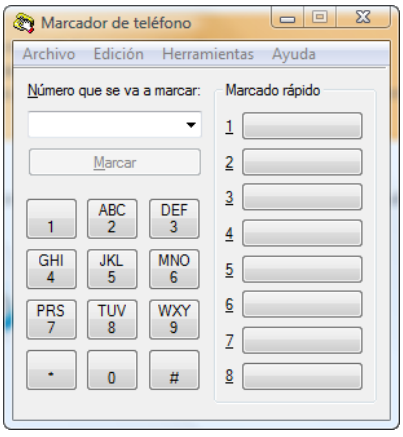
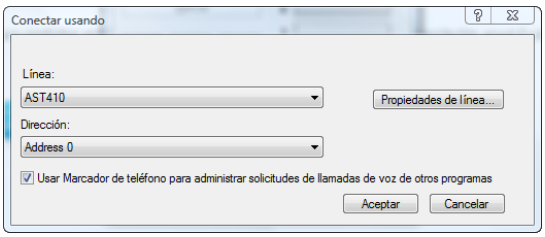
Evolution requiere también el componente opcional "CISCO Wave Driver". Para instalar este componente primero debe haber completado la instalación del CiscoTSP y posteriormente seguir las instrucciones "Installing the Wave Driver" incluidas en el documento "ciscotsp.txt" que la instalación de CiscoTSP ha copiado en el directorio donde éste se ha instalado.

16.5.8 CÓMO COMPROBAR EL CORRECTO FUNCIONAMIENTO DE CISCOTSP

Comprueba el correcto funcionamiento del conjunto CiscoTSP con la utilidad Windows dialer.exe

Esta aplicación permite realizar una llamada entre dos extensiones, a través de TAPI.

Cómo comprobar el correcto funcionamiento del conjunto TAPI / CiscoTSP

1	Desde el menú de inicio Windows, opción "ejecutar", ejecuta la utilidad "dialer.exe"	
2	Aparecerá el diálogo "Conectar usando". En caso contrario acceder a él mediante el menú "Herramientas | conectar usando" y seleccionar la línea correspondiente a una extensión que hayamos configurado en CISCO, p.ej: 410	

3	En el “dialpad” telefónico marca una extensión de destino, p. ejemplo: 412
4	Cuando pulses “marcar” debería generarse una llamada entre la extensión de origen (410) ya la extensión de destino (412).

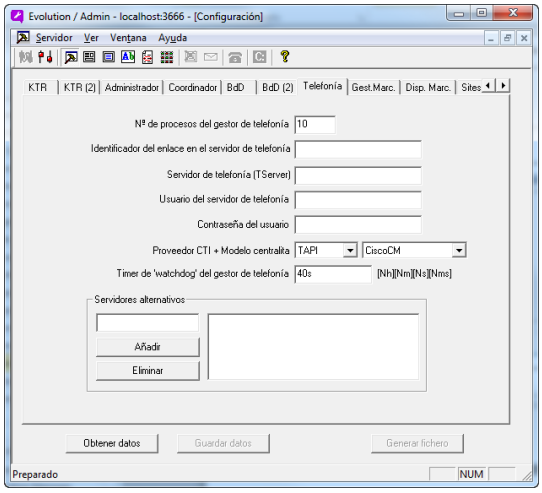
16.5.9 CÓMO CONFIGURAR EL ENLACE EVOLUTION AL CISCO TAPI

A través de Evoadmin.exe se deberán configurar los siguientes **parámetros de telefonía:**

Parámetro	Valor	Ejemplos
Identificador del enlace en el servidor de telefonía	vacío.	
Servidor de telefonía Tserver	Vacío	
Usuario y contraseña del servidor de telefonía	Vacío	
Proveedor CTI + Modelo centralita	TAPI / CiscoCM	TAPI / CiscoCM

Configuración de telefonía en evoadmin

Ejemplo de configuración en Evoadmin


Evolution / Admin - localhost:3666 - [Configuración]
Servidor Ver Ventana Ayuda
KTR KTR (2) Administrador Coordinador BdD BdD (2) Telefonía Gest.Marc. Disp. Marc. Sites
Nº de procesos del gestor de telefonía 10
Identificador del enlace en el servidor de telefonía
Servidor de telefonía (TServer)
Usuario del servidor de telefonía
Contraseña del usuario
Proveedor CTI + Modelo centralita TAPI CiscoCM
Timer de 'watchdog' del gestor de telefonía 40s [Nh][Nm][Ns][Nms]
Servidores alternativos
Añadir
Eliminar
Obtener datos
Guardar datos
Generar fichero
Preparado
NUM

16.5.10 CÓMO CONFIGURAR LOS DISPOSITIVOS DE MARCACION EN EVOADMIN

A través de Evoadmin.exe se deberán configurar los dispositivos de marcación para que correspondan con los Cisco CTI Ports administrados.

Administre la lista de dispositivos de marcación.

1. Ejecute y conéctese con evoadmin.exe
2. Configuración, Dispositivos de Marcación (Disp. Marc), Para añadir un dispositivo de marcación informe el parámetro “dispositivo” (ej: dispositivo=500),desmarque “asociado a tal” y pulse “Añadir”
3. Cuando termine de administrar los dispositivos pulse Guardar datos

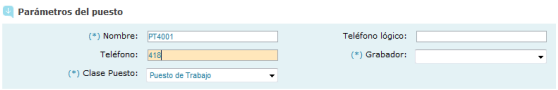
Ahora debemos administrar asociar estos dispositivos al módulo “servidor de dispositivos de marcación”.

1. Ejecute y conéctese con evoadmin.exe
2. Configuración → Gestor de Marcadores (GestMarc.), seleccione el servidor de dispositivos de marcación de la lista de servidores, pulsando en su Identificador. Pulse “Quitar” para pasar este servidor a ‘off-line’. Nota: por defecto solo existe uno servidor de marcación, cuyo identificador es “Dialer”.
3. Pulse “Dispositivos” para editar la lista de dispositivos disponibles para marcación. Edite la lista añadiendo todos los dispositivos que requiera. Guarde la selección de dispositivos con OK.
4. Pulse el botón “Añadir” en el diálogo de “Gest Marc.” para pasar el servidor a ‘on-line’ de nuevo.
5. Pulse Guardar datos.

16.5.11 CÓMO CONFIGURAR EL MÓDULO ICR DIALER DAEMON (EVODIALERSERVER)

Configuración del Servidor de Marcación con CISCO CM usando “CTI Ports”	
1	Evolution\Server\DialerParam.exe
2	Indicar la Máquina donde está instalado el Servidor de Marcación y pulsar Obtener Datos. Ej: “Maquina de Dialer”: “.” (un punto, indicando local)
3	En la pestaña DialerGlobal: > **Module** escribir el número 70 que es el correspondiente al tipo **TapiCiscoCM**.
4	Y pulsamos Guardar Datos.
5	Los cambios tendrán efecto en cuanto reinicie el servicio ICR Dialer Daemon

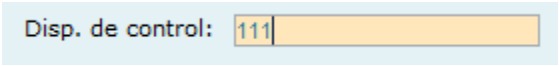
16.5.12 CÓMO CONFIGURAR USUARIOS Y PUESTOS EN EVOLUTION MANAGER

Configuración Manager		
1	Administración | Puestos	Informe el número de la extensión SIP en el parámetro “teléfono”. Deje vacío el “teléfono lógico” Ej: teléfono: 410 
2	Administración | Usuarios	Parámetros de usuario “login ACD” y “password ACD”: vacíos

16.5.13 CÓMO CONFIGURAR CAMPAÑAS DBR EN EVOLUTION MANAGER

Configuración Manager (configuración DBR)		
3	Administración | Campañas | Estrategias	En la lista de campañas seleccione “Ver Estrategias”, y administre una o más estrategias de encaminamiento. Ej: Estrategia de encaminamiento de tipo “DBR estático” que ofrece las llamadas a la cola de la campaña “Servicio técnico teléfono”

4	Administración | Campañas | Conectores DBR	En la lista de campañas seleccione “Ver Conectores DBR”, y administre un nuevo conector para cada CTI Route-Point CISCO. Evolution establecerá una asociación CTI con el dispositivo CTI Route Point especificado en la URL, y tratará las llamadas ofrecidas a este dispositivo aplicando la estrategia asignada. La estrategia determina la campaña, prioridades y otros atributos. Evolution ejecuta la estrategia de encaminamiento especificada en el conector o aquella cuyo DN coincida con el `route-point` de la llamada Ej: Para controlar el dispositivo Cisco CTI Route-Point 111 especifique URL=`ciscocm://?device=111` **Parámetros generales** ID: 100000004 (*) Nombre: cisco111 Estado: Activo Estrategia: 100000001 - 111 (*) URL: ciscocm://?device=111
5	Administración | Campañas	En la sección “Routing” seleccione la opción “Evolution DBR-Server” Administre una o más estrategias de tipo DBR, asociándolas a la campaña.

		Si la campaña requiere marcación predictiva o progresiva, informe el parámetro de campaña “Disp. De control” con el DN correspondiente al cti `route point` Cisco que deberá tratar las llamadas predictivas de esa campaña. Si la campaña no usa marcación progresiva o predictiva puede dejar esta campo vacío Ej: Dispositivo de Control asociado al cti route point 111 
6	Administración | Servicios	Configure los servicios con campañas exclusivamente de tipo DBR.

16.5.13.1 OBSERVACIONES Y LIMITACIONES CONOCIDAS

1	Los dispositivos CISCO CTI PORT utilizan el códec G.711. Por ello deberán administrarse en una región que fuerce el uso de este tipo de códec.	De lo contario, y si no puede negociarse un códec común en ambos extremos de la llamada. pueden producirse cortes en las llamadas de marcador.

16.6 PANASONIC SERIE TDA/TDE

Recomendado: TAPI / PANASONIC KX-TDA TAPI SERVICE PROVIDER

Evolution soporta los siguientes tipos de campaña con PANASONIC KX KX-TDA TAPI SERVICE PROVIDER:

- Inbound switch based routing
- Outbound vp

Mediante un servidor externo con tarjetas Dialogic y software adicional es posible configurar campañas outbound predictivo/progresivo. Consulte a ICR.

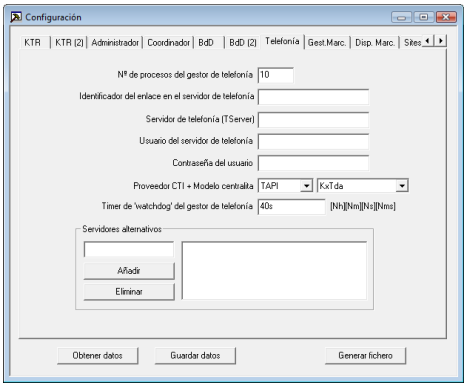
16.6.1 CÓMO INSTALAR EL CLIENTE PANASONIC KX-TDA TAPI SERVICE PROVIDER

Instale el componente “PANASONIC KX-TDA TAPI SERVICE PROVIDER” en el servidor Evolution, de acuerdo con las instrucciones del fabricante (PANASONIC).

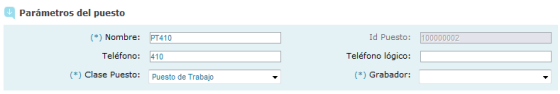
16.6.2 CÓMO CONFIGURAR EL ENLACE EVOLUTION A PANASONIC KX-TDA TSP

A través de Evoadmin.exe se deberán configurar los siguientes **parámetros de telefonía:**

Parametro	Valor	Ejemplos
Identificador del enlace en el servidor de telefonía	(vacío)	
Servidor de telefonía Tserver	(vacío)	
Usuario y contraseña del servidor de telefonía	(vacío)	
Proveedor CTI + Modelo centralita	TAPI / KXTDA	TAPI / KXTDA

Configuración de telefonía en evoadmin	
Ejemplo de configuración en Evoadmin	

16.6.3 CONFIGURACIONES DE EVOLUTION MANAGER

Configuración Manager		
1	Administración | Puestos	Informe el número de la extensión en el parámetro “teléfono” Deje vacío el “teléfono lógico” Ej: teléfono: 410 
2	Administración | Usuarios	Deje vacios los campos “login ACD” y “password ACD”.
3	Administración | Campañas	En la sección “Routing” seleccione la opción “switch-based” Evolution determina que las llamadas inbound pertenecen a una campaña cuando el `calleddevice` de la llamada coincide con el DN de una estrategia DNIS asociada a la campaña.

En Panasonic KX normalmente dicho DN coincide con el número asignado al UCD que atiende las llamadas.

En la sección “Routing” administre una o más estrategias de tipo de encaminamiento ‘DNIS’, y asígnela a la campaña.

Ej: Estrategia de encaminamiento tipo DNIS con DN: 100 y asociada a la campaña “atención al cliente”

Informe el parámetro “Disp. De control” con el UCD que deberá atender las llamadas predictivas/progresivas. Si la campaña no usa marcación progresiva o predictiva puede dejar este campo vacío. Para generar llamadas con marcación progresiva o predictiva se requiere un servidor adicional con tarjetas DIALOGIC, no incluido.

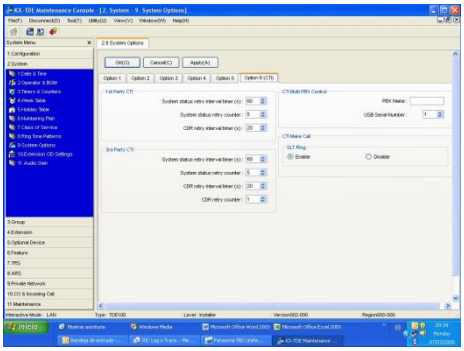
Ej: Dispositivo de control 601:

16.6.4 NOTAS TÉCNICAS

Instalación y configuración de PANASONIC serie TDA/TDE	
1	Incluir tarjeta la DISA para mensajes de cola de llamadas. Requiere Teléfonos ESPECIFICOS / DIGITALES Interfaz TAPI a través de ETHERNET

	(TSP Panasonic v2.0.2.14 o superior)	
2	Activar wrap-up time 5 segundos	
3	Deshabilitar “llamadas en espera”	**Evitar** que cuando una extensión tenga una llamada en hold se pueda recibir una segunda llamada de ACD
4	Programación de grupos como ACD/UCD	No funciona con timbrado a todo el grupo en forma simultanea
5	NO UTILIZAR Conexión en doble puerto digital DXDP	Los teléfonos conectados en doble puerto digital (DXDP) no están disponibles en CTI/TAPI
6	Procedimiento para que las llamadas entre agentes no se restrinjan por “No Molesten” (Do-Not-Disturb)3.	Los teléfonos del CallCenter deben estar en una misma clase de servicio que tengan activado el "ignorar NO MOLESTEN". Dar de alta todos los teléfonos de esta clase en EVOLUTION, para que sean llamadas de agente-agente (y no de campaña). Para hacer las llamadas consultivas a un agente utilizar el siguiente procedimiento: Llamar a la extensión del AGENTE en cuestión. Aparece en el Display del teléfono una indicación de ND (Do not Disturb) o NM (No Molesten) Presionar en el teclado del teléfono el numero 1 (uno)
7	Para hacer login/logout/ready/not-ready en una configuración con KX-TDA, Evolution ejecuta makeCall(·) con secuencias de dígitos, equivalentes a las que se podrían pulsar en la extensión.	Estas son las secuencias estándar, y se sugiere revisar que en la configuración de KX-TDA sean las mismas. En todo caso las secuencias que utiliza evolution se pueden editar creando o modificando las siguientes claves de

[3] Evolution utiliza el estado Do-Not-Disturb en NO-DISPONIBLE

	Cuando un agente se conecta se envía la siguiente secuencia de login: **LOGIN: *7361** Inmediatamente después de login también se introduce la secuencia de ready: **READY: *7350** Posteriormente se utiliza el flag de DO-NOT-DISTURB on/off cuando es necesario, para gestionar el estado de los agentes y evitar que reciban llamadas cuando el agente no esté en situación de disponible. Finalmente, cuando el agente se desconecta, se envía la secuencia de logout: **LOGOUT: *7360**	registry en evoserver: [HKEY_LOCAL_MACHINE\SOFTWARE\ICR\PbxApi32\Global] "Seq4NotReady"="*7351" "Seq4Ready"="*7350" "Seq4Logout"="*7360" "Seq4Login"="*7361"
8	Si utiliza extensiones analógicas recomendamos active la opción **SLT RING = ENABLE** Vea “System Options” de KX-TDA/TDE Maintenace Console	

16.6.4.1 LIMITACIONES CONOCIDAS DE PANASONIC KX-TDA

1	En algunas situaciones las llamadas entrantes en cola ACD/UCD no se ofrecen a la extensión cuando ésta desactiva el DND.	

16.7 ALCATEL OMNI PCX ENTERPRISE, ALCATEL 4400

Recomendado: CTConnect 7.5

Evolution soporta los siguientes tipos de campaña con OMNI PCX ENTERPRISE, ALCATEL 4400:

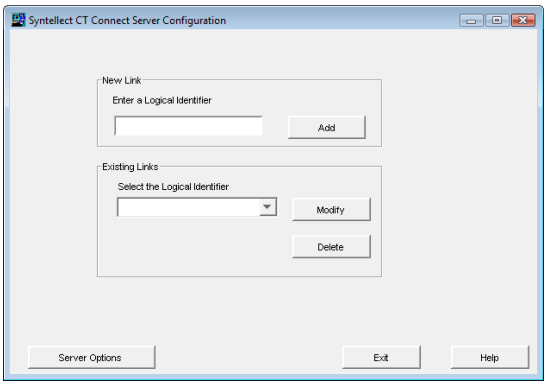
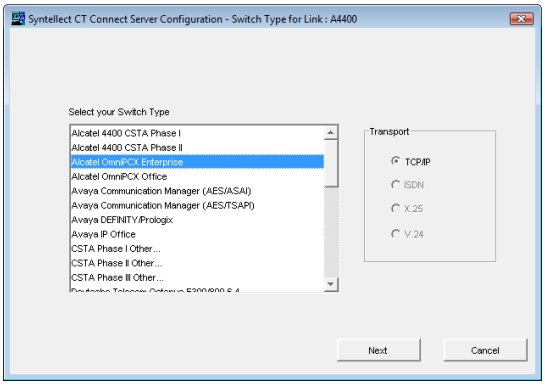
- Inbound switch based routing
- Outbound vp

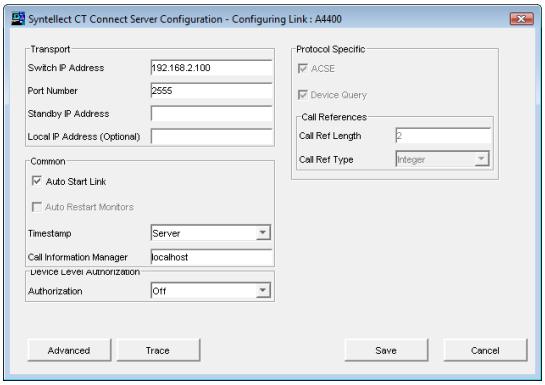
Mediante un servidor externo con tarjetas Dialogic y software adicional es posible configurar campañas outbound predictivo/progresivo. Consulte a ICR.

16.7.1 CÓMO CONFIGURAR EL SERVIDOR CTCONNECT SERVER

Instale el componente “Syntellect CTConnect server 7.5” de acuerdo con las instrucciones del fabricante (Syntellect). Este software puede instalarse en el mismo servidor que Evolution o en un servidor independiente. Tenga en consideración los requerimientos específicos de “Syntellect CTConnect server 7.5”.

Para configurar un enlace a ALCATEL OMNIPCX ENTERPRISE

1	Ejecutar la aplicación “Menú de Inicio | Syntellect CT Connect | Configuration Program” Crear un LINK, especificando un LOGICAL IDENTIFIER adecuado. P.ej: “A4400”	
2	Seleccionar el switch Type “ALCATEL OmniPCX Enterprise”	

3	Configurar los parámetros adecuados para el link administrado en Alcatel. Establezca el “Switch IP Address” correspondiente al servidor Alcatel OmniPCX Enterprise.	
4	Si es necesario, reiniciar el servidor, comprobar que el servicio Syntellect CT Connect está en iniciado y en modo modo inicio automatico	
5	Podemos comprobar el nuevo link: ▪ Aplicación “Menú de Inicio | Syntellect CT Connect | Control Program” ▪ Informar el Parametro CurrentServer y botón [REFRESH] debe mostrar el Logical Identifier, con el correspondiente Link State (UP)	

16.7.2 CÓMO INSTALAR EL CLIENTE SYNTELLECT CT CONNECT CLIENT

Instale el componente “Syntellect CT Connect client” en el servidor Evolution, de acuerdo con las instrucciones del fabricante (Syntellect).

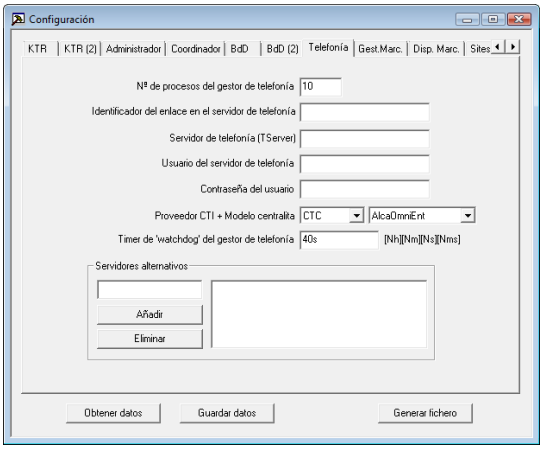
16.7.3 CÓMO CONFIGURAR EL ENLACE EVOLUTION AL SWITCH OMNIPCX

A través de Evoadmin.exe se deberán configurar los siguientes **parámetros de telefonía:**

Parametro	Valor	Ejemplos
Identificador del enlace en el servidor de telefonía	Corresponde al “LOGICAL ID” configurado en CTConnect server	“A4400”
Servidor de telefonía Tserver	Dirección IP del servidor CTConnect	192.168.1.105 o localhost
Usuario y contraseña del servidor de telefonía	(vacío)	
Proveedor CTI + Modelo centralita	CTC / AlcaOmniEnt	CTC / AlcaOmniEnt

Configuración de telefonía en evoadmin

Ejemplo de configuración en Evoadmin



16.7.4 CÓMO CONFIGURAR EL MÓDULO ICR DIALER DAEMON (EVODIALERSERVER)

NOTA IMPORTANTE: Para campañas con marcación progresiva o predictiva se requiere un servidor adicional con tarjetas DIALOGIC, no incluido.

Configuración del Servidor de Marcación con ALCATEL OmniPCX Enterprise

1 Iniciar c:\ICR\Evolution\Server\DialerParam.exe

2 Indicar la Máquina donde está instalado el Servidor de Marcación y pulsar Obtener Datos.

Ej: “Maquina de Dialer”: “.” (un punto, indicando local)

3 En la pestaña DialerGlobal:

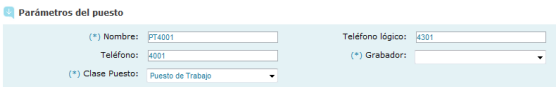
> **Module** escribir el número 47 que es el correspondiente al tipo CtcAlcaOmniEnt.

>**MainLinkID** escribir el mismo valor que hayamos indicado en el parámetro “Identificador del enlace en el servidor de telefonía” en evoadmin. P.ej: “AS4400”

>**MainServerID** nombre del servidor de telefonía. Escribir el mismo valor que hayamos indicado en el parámetro “Servidor de telefonía Tserver” en evoadmin.

	P.ej: “192.168.1.110” >**MainLogin/MainPwd** usuario/contraseña. Dejar vacios.
4	Y pulsamos Guardar Datos.

16.7.5 CONFIGURACIONES DE EVOLUTION MANAGER

Configuración Manager		
1	Administración | Puestos	Informe el número extensión (DN) de la extensión en el parámetro “Teléfono” Para usar usar configuración con “Agente Flotante” informe el valor “#FLO” como “Teléfono lógico”. Así en cuanto el agente se conecte el servidor monitorizará el DN correspondiente al agentACD configurado en el usuario Evolution. Ej: teléfono: 4001, teléfono lógico: #FLO 
2	Administración | Usuarios	Informe en los parámetros de ACD el “login ACD” y “password ACD” administrados en ALCATEL. Cuando el agente Evolution se conecte, se utilizarán estos parámetros para efectuar el login ALCATEL y se monitorizará el DN correspondiente al agentID. Ej: Login ACD: 50001
3	Administración | Campañas	En la sección “Routing” seleccione la opción “switch-based” Evolution determina que las llamadas *inbound* pertenecen a una campaña cuando el `calleddevice` de la llamada coincide con el DN de una estrategia DNIS asociada a la campaña.

Administre una o más estrategias de tipo DNIS, asociadas a la campaña.

En la sección “Routing” administre una o más estrategias de tipo de encaminamiento ‘DNIS’, y asígnela a la campaña.

Informe el parámetro DN del DNIS con el número de PILOT ACD que entrega las llamadas *inbound*.

Ej: Estrategia de encaminamiento tipo DNIS con DN: 100 y asociada a la campaña “atención al cliente”

Informe el parámetro “Disp. De control” con el PILOT ACD que deberá generar las llamadas predictivas/progresivas. Si la campaña no usa marcación progresiva o predictiva puede dejar esta campo vacío

Ej: Disp. De control: 30001

16.7.6 NOTAS TÉCNICAS

Instalación y configuración de Alcatel OXE, ALCATEL 4400	
1	Active el wrap-up time con un valor de 5 segundos

16.8 IP-PBX ASTERISK

Recomendado: TAPI ActivaTSP

Evolution soporta los siguientes tipos de campaña con IP-PBX Asterisk:

- Inbound switch based routing
- Inbound DBR
- Outbound vp
- Outbound predictivo/progresivo (switch-based)
- Outbound predictivo/progresivo (DBR)

Para los modos switch-based, Evolution hace uso de colas ACD Asterisk.

16.8.1 CONFIGURACIÓN CERTIFICADA

La siguiente es la lista de equipos y software que se utilizó para la validación y certificación de Evolution en un entorno Asterisk:

Equipamiento	Software
Asterisk	Asterisk 1.8.11-cert10
IP Phone	IP softphone: ▪ Xlite ▪ Zoiper SIP Phone: ▪ SNOM 320 ▪ Linksys SPA-941
Asterisk TAPI Service Provider	ActivaTSP 1.8.9
Evolution 10.0	Windows W2008 Server R2 SQL server 2008 Express

Tambien se ha comprobado el funcionamiento con otras versiones de Asterisk:

- Asterisk 1.4
- Asterisk 1.6

Para instrucciones de instalación con Elastix ver el apartado correspondiente.

16.8.2 CÓMO HABILITAR LA INTERFAZ DE CONEXIÓN AMI EN ASTERISK

Para acceder a la línea de comandos de Linux puede conectarse por ssh desde Windows con Putty (http://www.chiark.greenend.org.uk/~sgtatham/putty/download.html).

Desde la línea de comandos del servidor editar /etc/asterisk/manager.conf y crear la sección `[evolution]`:

Para Asterisk 1.2 y 1.4:

```
[evolution]
secret = bomber
#deny=
permit=0.0.0.0/0.0.0.0
read = system,call,log,verbose,command,agent,user
write = system,call,log,verbose,command,agent,user
```

Para Asterisk 1.6 y 1.8:

```
[evolution]
secret = bomber
#deny=
permit=0.0.0.0/0.0.0.0
read = system,call,log,verbose,command,agent,user,originate
write = system,call,log,verbose,command,agent,user,originate
```

Nota: Observe que asterisk 1.6 y 1.8 requiere el permiso adicional `originate`.

Para que los cambios tengan efecto reinicie el servicio, ejecutando desde la línea de comandos: /etc/init.d/asterisk restart

16.8.3 CÓMO CONFIGURAR LAS EXTENSIONES

Para configurar extensiones, desde la línea de comandos del servidor editar /etc/asterisk/manager.conf sip.conf (en estas notas utilizaremos las extensiones de ejemplo 411 y 412):

sip.conf

```
 [411]
username=411
type=friend
record_out=Adhoc
record_in=Adhoc
qualify=no
port=5060
nat=never
mailbox=411@device
host=dynamic
dtmfmode=rfc2833
context=default
canreinvite=no
callerid=user1 <411>

[412]
username=412
type=friend
record_out=Adhoc
record_in=Adhoc
qualify=no
port=5060
nat=never
mailbox=412@device
host=dynamic
dtmfmode=rfc2833
context=default
```

```
        canreinvite=no
        callerid=user2 <412>
```

Editar el fichero extensions.conf, añadiendo un nuevo contexto:

extensions.conf

```
    [from-internal]
      …/…
      exten => _4XX,1,dial(SIP/${EXTEN})
```

Conectar sus teléfonos SIP a la LAN, configurarlos para conectarse al servidor ASTERISK y comprobar que se pueden llamar entre ellos.

16.8.4 CÓMO CONFIGURAR LAS COLAS ACD ASTERISK

Configurar las Queue Asterisk necesarias.

Edite `queues.conf` y parametrícelas a partir del siguiente ejemplo para la cola 100:

queues.conf

```
    [100]
      announce-frequency=0
      timeout=15
      strategy=rrmemory
      retry=5
      queue-youarenext=
      queue-thereare=
      queue-thankyou=queue-thankyou
      queue-callswaiting=
      music=default
      monitor-join=yes
      monitor-format=
```

```
maxlen=0

leavewhenempty=no

joinempty=yes

eventwhencalled=no

eventmemberstatus=no

context=

announce-holdtime=no

wrapuptime=0

autofill=yes
```

Edite el fichero `extensions.conf` para que las extensiones correspondientes a las colas ACD controladas por Evolution informen el campo CALLERID(name) adecuadamente. Puede partir del siguiente ejemplo para la cola 100:

extensions.conf

```
[from-internal]

  …/…

  exten => 100,1,Set(CALLERID(name)=100:${CALLERID(name)})

  exten => 100,n,Queue(100|t||)
```

Nota: ActivaTSP utiliza la variable `CALLERID(name)` para identificar las llamadas de cola ACD. Se requiere que el contenido de dicha variable sea de la forma <num_queue>:<contenido>

16.8.5 CÓMO CONFIGURAR UNA EXTENSIÓN TIPO ROUTE-POINT

En una configuración con campañas DBR deberá configurar una o más extensiones asterisk como “route-point” para que las llamadas puedan ser controladas por el módulo EvoRouter. Si utiliza configuración tipo “switch-based” no es necesario que administre ningún route-point.

Al configurar extensiones tipo “route-point” la configuración resultante puede ser una combinación de las siguientes:

- Cada ruta de llamadas inbound se encaminan a una extensión asterisk (Route-Point) diferente. El servidor DBR ejecutará aquella estrategia de encaminamiento cuyo DN coincida con el route-point (ej: 100)
- Varias rutas de llamadas inbound se encaminan a una misma extensión asterisk (Route-Point). El servidor DBR ejecutará aquella estrategia de encaminamiento cuyo DN coincida con el valor de la variable RDNIS de la llamada en asterisk.

Para crear una extensión asterisk que actúe como “route-point”:

1- Administre el dialplan asterisk y cree una nueva extensión, editando extensions.conf o extensions_custom.conf
2- Configure el dialplan de la nueva extensión para que ejecute una llamada FastAGI al módulo EvoRouter del servidor.
    a. P.ej, si evorouter está escuchando en la dirección `192.168.0.177`
    ```
    exten => 111,1,AGI(agi://192.168.0.177/EvoRouter);
    ```
3- Administre el dialplan asterisk para que encamine hacia la nueva extensión las rutas de entrada deseadas.

Por ejemplo, para crear una extensión 111 tipo route-point que se conecte al módulo EvoRouter en la dirección IP 192.168.0.177:

Extensions_custom.conf

```
exten => 111,1,AGI(agi://192.168.0.177/EvoRouter);
```

Nota: Se recomienda que a continuación del comando AGI() establezca la secuencia de pasos adecuada para tratar escenarios de fallo de enrutamiento, por ejemplo, desviar la llamada a otro destino o extensión de emergencia.

En versiones de Asterisk 1.6 o superiores es posible configurar el modo compatibilidad con versiones anteriores, que afecta a los separadores de opciones usados en AGi y FastAGI.

Puede consultarse si el modo compatibilidad está activado si en el fichero de configuración Asterisk.conf está establecido el parámetro res_agi=1.4 en la sección [compat] o dicho parámetro no existe.

En estos casos sera necesario indicar el parámerto adicional “CompatResAGIVersion=1.4” en la definición del route-point, por ejemplo:

Extensions_custom.conf

```
exten => 111,1,AGI(agi://192.168.0.177/EvoRouter?
CompatResAGIVersion=1.4);
```

16.8.6 EJEMPLO DE UN FRAGMENTO DE DIAL PLAN MÍNIMO

En determinadas situaciones puede ser conveniente establecer un dialplan mínimo, por ejemplo para diagnosticar y resolver problemas.

Tome como referencia los siguientes fragmentos de dialplan

Ejemplo para extensiones de agente 4XX

```
;SIP AGENTS TEST
```

```
exten => _4XX,1,Dial(SIP/${EXTEN})

exten => _4XX,n,Hangup()
```

Ejemplo para colas ACD 10X

```
;QUEUE TEST

exten => _10X,1,Set(CALLERID(name)=${EXTEN}:${CALLERID(name)})

exten => _10X,n,Queue(${EXTEN},t,,)
```

Ejemplo para routepoint DBR

```
;ROUTEPOINT TEST

exten => 111,1,AGI(agi://192.168.0.177/EvoRouter);
```

16.8.7 CÓMO INSTALAR ACTIVATSP (TAPI SERVICE PROVIDER)

Instalar y configurar Activa TSP en el servidor Evolution.

NOTA: Se requiere ActivaTSP 1.8.9. Si utiliza SO Windows Server 2008 R2 64 bits instale la versión x64 de ActivaTSP.

Descargar e instalar Activa TSP (http://activa.sourceforge.net/)

Configurar el TSP para que pueda controlar las extensiones de los agentes y las colas: inicio → Panel de control → Opciones de teléfono y modem → Opciones Avanzadas → ActivaTSP for Asterisk

Incluya las extensiones y las colas ACD que desea controlar en “Line DN”. Puede utilizar una lista separada por comas, como por ejemplo DN=”410-419, 100, 101”.

NOTA: ActivaTSP utiliza recursos para cada DN especificado en “Line DN”. Mantenga la lista de DN tan reducida como sea posible.

NOTA: No es necesario incluir las extensiones de agente que se configuren para usar el softphone integrado.

Asegúrese de que el parámetro “Line Prefix” = “AST”

Configure el usuario y password de acceso a asterisk manager interface (AMI) según anteriormente haya configurado `manager.conf`. Si ha utilizado los valores de ejemplo de las instrucciones los parámetros serán los siguientes: `user=evolution, secret= bomber`

Si quiere forzar un idioma para las llamadas iniciadas por CTI puede establecer el campo Orig. Variable = “CHANNEL(language)=es”

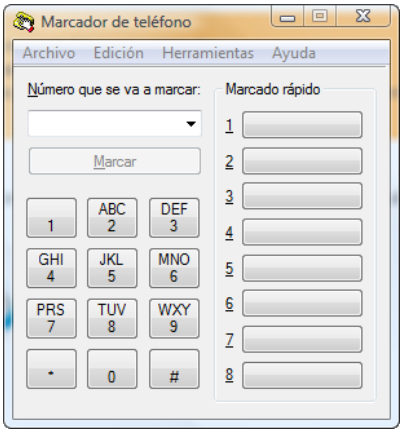
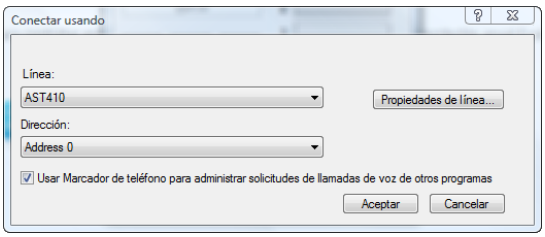
Ejemplo de parámetros ActivaTSP:

Line DN = “100-101,410-419”
Line Prefix = “AST”
Orig. Variable = “CHANNEL(language)=es”
Outgoing = “from-internal”
Agent = “from-internal”
Host IP = <*Entrar dirección IP de /ElastixTrixbox*>
Port = “5038”
User = “evolution” (Nota: corresponde a la sección de usuario [evolution], especificado en manager.conf)
Password = “bomber” (Nota: corresponde al ‘secret’ especificado en manager.conf)

Tras guardar los cambios, debes reiniciar el servidor Windows 2003/2008 para asegurar que éstos tengan efecto.

16.8.8 CÓMO COMPROBAR EL CORRECTO FUNCIONAMIENTO DEL CONJUNTO ACTIVATSP / ASTERISK

Cómo comprobar el correcto funcionamiento del conjunto activatsp / asterisk

1	Desde el menú de inicio Windows, opción “ejecutar”, ejecuta la utilidad “dialer.exe”	
2	Aparecerá el diálogo “Conectar usando”. En caso contrario acceder a él mediante el menú “Herramientas | conectar usando” y seleccionar la línea correspondiente a una extensión que hayamos configurado en asterisk, p.ej: AST410	
3	En el “dialpad” telefónico marca una extensión de destino, p. ejemplo: 412	

4	Cuando pulses “marcar” debería timbrar en primer lugar la extensión de origen (410), y en cuanto la descuelgues, la llamada progresará hacia su destino (412).

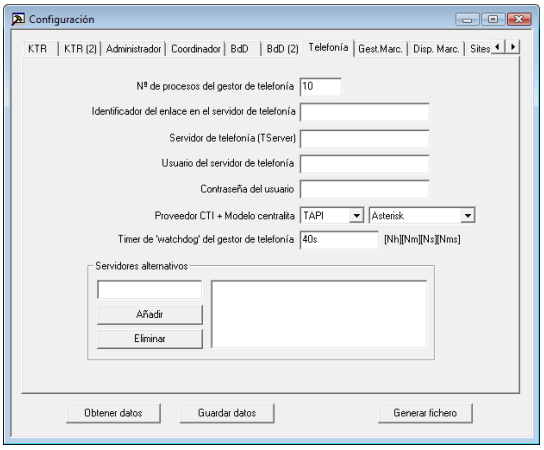
16.8.9 CÓMO CONFIGURAR EL ENLACE EVOLUTION AL SERVIDOR ASTERISK

A través de Evoadmin.exe se deberán configurar los siguientes **parámetros de telefonía:**

Parametro	Valor	Ejemplos
Identificador del enlace en el servidor de telefonía	(Vacío)	
Servidor de telefonía Tserver	(Vacío)	
Usuario y contraseña del servidor de telefonía	(Vacío)	
Proveedor CTI + Modelo centralita	TAPI/ASTERISK	Ej: TAPI/ASTERISK

Configuración de telefonía en evoadmin

Ejemplo de configuración en Evoadmin



16.8.10 CÓMO CONFIGURAR EL MÓDULO ICR DIALER DAEMON (EVODIALERSERVER)

Configuración del Servidor de Marcación con ASTERISK	
1	Iniciar c:\ICR\Evolution\Server\DialerParam.exe
2	Indicar la Máquina donde está instalado el Servidor de Marcación y pulsar [Obtener Datos]. Ej: “Maquina de Dialer”: “.” (un punto, indicando local)
3	En la pestaña DialerGlobal: > **Module** escribir el número 66 que es el correspondiente al tipo TapiAsterisk >**MainLinkID** (vacío) >**MainServerID** (vacío) >**MainLogin/MainPwd** (vacío)
4	Y pulsamos [Guardar Datos].

16.8.11 CÓMO ADMINISTRAR LOS DISPOSITIVOS DE MARCACIÓN EN EVOADMIN

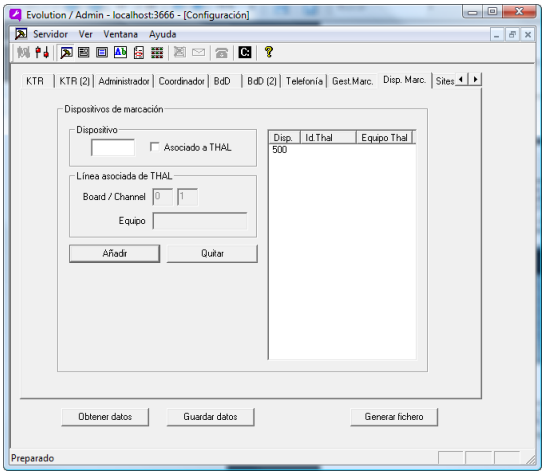
En el caso de utilizar IP-PBX Asterisk los dichos dispositivos de marcación Evolution son dispositivos “lógicos”, y no corresponden a DN o dispositivos reales.

No obstante debe administrar un número suficiente y adecuado de dispositivos de marcación en Evoadmin, para soportar los procesos de marcacion.

Configuración de Dispositivos de Marcación en evoadmin

1 Ejecute evoadmin.exe, indique el *password* para operaciones restringidas, acceda al diálogo de “Configuración”, TAB “Disp. Marcador” y edite la lista de dispositivos de marcación.

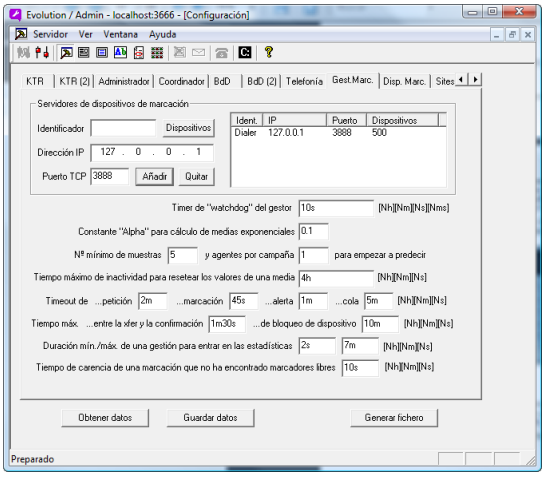
Pulse Guardar Datos.



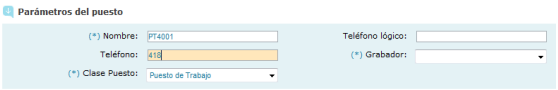
2 En el TAB “Gest. Marc.” pase a “off-line” el marcador seleccionando el identificador del “servidor de dispositivos de marcación” y pulsando el botón “Quitar”.

Pulse “Dispositivos”, edite la lista de dispositivos añadiéndole todos los dispositivos correspondientes a wave ports. Una vez editados pulse “Añadir” para pasar a “on-line”.

Pulse Guardar Datos.


Evolution / Admin - localhost:3666 - [Configuración]
Servidor Ver Ventana Ayuda
KTR KTR (2) Administrador Coordinador BdD BdD (2) Telefonía Gest.Marc. Disp. Marc. Sites
Servidores de dispositivos de marcación
Identificador
Dispositivos
Dirección IP 127 . 0 . 0 . 1
Puerto TCP 3888
Añadir
Quitar
Ident. IP Puerto Dispositivos
Dialer 127.0.0.1 3888 500
Timer de "watchdog" del gestor 10s [Nh][Nm][Ns][Nms]
Constante "Alpha" para cálculo de medias exponenciales 0.1
Nº mínimo de muestras 5 y agentes por campaña 1 para empezar a predecir
Tiempo máximo de inactividad para resetear los valores de una media 4h [Nh][Nm][Ns]
Timeout de ...petición 2m ...marcación 45s ...alerta 1m ...cola 5m [Nh][Nm][Ns]
Tiempo máx. ...entre la xfer y la confirmación 1m30s ...de bloqueo de dispositivo 10m [Nh][Nm][Ns]
Duración mín./máx. de una gestión para entrar en las estadísticas 2s 7m [Nh][Nm][Ns]
Tiempo de carencia de una marcación que no ha encontrado marcadores libres 10s [Nh][Nm][Ns]
Obtener datos
Guardar datos
Generar fichero
Preparado

16.8.12 CÓMO CONFIGURAR USUARIOS Y PUESTOS EN EVOLUTION MANAGER

Configuración Manager		
1	Administración | Puestos	Informe el número de la extensión SIP en el parámetro “teléfono” Deje vacío el “teléfono lógico” Ej: teléfono: 410 
2	Administración | Usuarios	Parámetros de usuario “login ACD” y “password ACD”: vacíos

16.8.13 CÓMO CONFIGURAR CAMPAÑAS SWITCH-BASED EN EVOLUTION MANAGER

Configuración Manager (configuración switch-based routing)		
3	Administración | Campañas	En la sección “Routing” seleccione la opción “switch-based” Evolution determina que las llamadas *inbound* pertenecen a una campaña cuando el `calleddevice` de la llamada coincide con el DN de una estrategia DNIS asociada a la campaña. Administre una o más estrategias de tipo DNIS, asociadas a la campaña. En asterisk el valor de DNIS debe coincidir con el DN de la QUEUE ACD Asterisk que entregue las llamadas a los agentes. En la sección “Routing” administre una o más estrategias de tipo de encaminamiento ‘DNIS’, y asígnela a la campaña.

		Ej: Estrategia de encaminamiento tipo DNIS con DN: 100 y asociada a la campaña “atención al cliente” En la administración de campaña informe el parámetro “Disp. De control” con el QUEUE ACD Asterisk que deberá generar las llamadas predictivas/progresivas. Si la campaña no usa marcación progresiva o predictiva puede dejar este campo vacío

4	Administración | Servicios	Configure un servicio con un ACD que coincida con el correspondiente QUEUE ACD asterisk
		
		Cuando un agente se conecte a Evolution utilizando un Puesto de Trabajo con extensión, el servidor realizará login de esta extensión a la QUEUE ACD asterisk correspondiente al servicio.
		
		Puede utilizar secuencias de conexión para hacer ‘login’ / ‘logout’ a colas adicionales.
		
		Las secuencias soportadas son las siguientes:
		
		LOGIN:
		`#FEATURE=Login#QUEUE=<queue>`
		
		LOGOUT:
		`#FEATURE=Logout#QUEUE=<queue>`
		
		Si tenemos varias campañas adicionales, podemos separar las secuencias con punto y coma. Por ejemplo, si queremos hacer login en las colas 500 y 501 haríamos:
		
		Secuencia de conexión:
		#FEATURE=Login#QUEUE=500;#FEATURE=Login#QUEUE=501
		Secuencia de desconexión:
		#FEATURE=Logout#QUEUE=500;#FEATURE=Logout#QUEUE=501

Recuerde que en la secuencia de conexión/desconexión no es necesario incluir la cola de la campaña que coincida con el DN del servicio.

16.8.14 CÓMO CONFIGURAR DEVELOPER SERVICE PARA SUBIR LOCUCIONES ASOCIADAS A LOS SCRIPTS DBR

Las opciones a configurar están relacionadas con el despliegue de DBR Scripts, por lo que únicamente es necesario modificar los parámetros en el caso de que se vaya a usar este tipo de estrategias.

Para configurar los parámetros tendrá que modificar el archivo web.config del directorio de instalación de Developer Service (por defecto: C:\inetpub\wwwroot\Evolution\DeveloperService). En la sección <appSettings> configure las siguientes claves:

```
<!-- Parametros SFTP para audios de Script DBR -->
<add key="SFTPHost" value="scm" />
<add key="SFTPUser" value="evolution" />
<add key="SFTPPort" value="22" />
<add key="SFTPPassword" value="bomber" />
<!-- Directorio raiz donde se ubicarán las locuciones de los DBRScripts  -->
<add key="SFTPRootSounds" value="/var/lib/asterisk/sounds" />
<!-- Directorio raiz donde se gestiona Music on hold -->
<add key="SFTPRootMoh" value="/etc/asterisk/icr"/>
<!-- Directorio fuente donde se encuentran los Scripts DBR -->
<add key="DBRScripts" value="Evolution/DBRScripts"/>
<!-- Puerto AMI para hacer el reload (el host es igual que el SFTPHost) -->
<add key="AMIPort" value="5038"/>
<!-- Usuario AMI -->
<add key="AMIUser" value="evolution"/>
<!-- Password AMI -->
<add key="AMISecret" value="bomber"/>
```

Para más información ver “12 Dynamic Business Router”

16.8.15 CÓMO CONFIGURAR CAMPAÑAS DBR EN EVOLUTION MANAGER

Configuración Manager (configuración DBR)		
1	Administración | Campañas	En la sección “Routing” seleccione la opción “Evolution DBR-Server” Evolution ejecuta la estrategia de encaminamiento cuyo DN coincida con el `route-point` de la llamada. La estrategia asigna la campaña, prioridades y otros atributos. Administre una o más estrategias de tipo DBR, asociadas a la campaña. Ej: Estrategia de encaminamiento tipo DBR estático con DN: 111 y asociada a la campaña “Servicio Técnico”

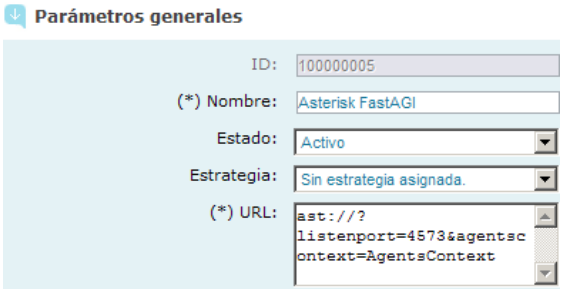
En la administración de campaña informe el parámetro “Disp. De control” con el DN correspondiente al `route-point` asterisk que deberá generar y tratar las llamadas predictivas de esa campaña.

Si la campaña no usa marcación progresiva o predictiva puede dejar esta campo vacío

2	Administración | Campañas | Conectores DBR	En la lista de campañas seleccione “Ver Conectores DBR”, y administre un nuevo conector para cada puerto FastAGI que se quiera publicar. Evolution, según el puerto (parámetro *listenport*), el contexto de los agentes (parámetro *agentscontext*) y el MusicOnHold (parámetro *moh*) especificado en la URL, atenderá las llamadas recibidas aplicando la estrategia asignada. La estrategia determina la campaña, prioridades y otros atributos. En caso de no asignar ninguna estrategia, Evolution escogerá de forma dinámica aquella cuyo DN coincida con el `route-point` de la llamada. Por defecto, el conector DBR se publica en el puerto 4573, usando el contexto para los agentes y MusicOnHold por defecto de Asterisk. El formato de configuración del conectorURL se especifica según: *Protocol://[UserInf@][[Host]:[Port]][/[Ruta][?[[Par*

amN]=[ValueN]]&…]]

Ej: Para publicar el conector DBR a través del puerto 4573 y contexto para los agentes "AgentsContext" especifique la URL= `ast://?listenport=4573&agentscontext=AgentsContext`



16.8.16 CÓMO CONFIGURAR MANAGER PARA SUPERVISAR CONVERSACIONES

Para poder escuchar e intervenir en las conversaciones de los agentes es necesario configurar la conexión con AMI en Manager.

Para configurar los parámetros tendrá que modificar el archivo web.config del directorio de instalación de Manager (por defecto: C:\inetpub\wwwroot\Manager). En la sección <appSettings> configure las siguientes claves:

```
<!-- Host AMI -->
<add key="AMIHost" value="scm" />
<!-- Puerto AMI -->
<add key="AMIPort" value="5038"/>
<!-- Usuario AMI -->
<add key="AMIUser" value="evolution"/>
<!-- Password AMI -->
<add key="AMISecret" value="bomber"/>
```

La opción de conferenciar no está disponible en versiones de Asterisk 1.4.x.

16.8.17 NOTAS TÉCNICAS

Instalación y configuración de Asterisk		
1	Los nombres de las extensiones y colas controlados por Evolution deben ser numéricos. Ejemplo: “100” o “410”	Los nombres alfanuméricos (ej: “my-SIP-phone”) no están soportados
2	El dialplan de las colas ACD (ACD queue) deben forzar un Caller-ID-Name (CIDName) que comience por el número de la cola seguido por dos puntos. Ejemplo: Si la ACD queue=100, se requiere CID name prefix= "100:"	ActivaTSP utiliza este prefijo en CID-Name para identificar a qué cola pertenecen las llamadas que se ofrecen a las extensiones de los agentes.
3	La conexión LAN entre Asterisk y ActivaTSP es crítica. Por ello se recomienda que dicha conexión se realice mediante una red dedicada.	En muchos casos puede ser aconsejable dotar a ambos servidores de dos tarjetas de red (NIC), dedicando una de ellas a esta red privada Asterisk/ActivaTSP. Otras recomendaciones son las siguientes: • Establecer el parámetro de Manager.conf:-writetimeout = 500 • Configurar los siguientes parametros de los adaptadores de red: 100 Mbps, full duplex, autoneg off
4	La política de distribución de llamadas de las colas ACD (ACD queues) recomendada es rrmemory (round-robin with memory).	Otros esquemas como por ejemplo “ring all” no están soportados y pueden generar eventos erróneos.

16.9 IP-PBX ASTERISK ELASTIX

Recomendado: TAPI ActivaTSP

Evolution soporta los siguientes tipos de campaña con IP-PBX Asterisk ELASTIX:

- Inbound switch based routing
- Inbound DBR
- Outbound vp
- Outbound predictivo/progresivo (switch-based)
- Outbound predictivo/progresivo (DBR)

Para los modos switch-based, Evolution hace uso de colas ACD Asterisk.

16.9.1 CONFIGURACIÓN CERTIFICADA

La siguiente es la lista de equipos y software que se utilizó para la validación y certificación de Evolution en un entorno Elastix (Asterisk):

Equipamiento	Software
Elastix (asterisk)	Elastix 1.6-12
IP Phone	IP softphone: ▪ Xlite ▪ Zoiper SIP Phone: ▪ SNOM 320 ▪ Linksys SPA-941
Asterisk TAPI Service Provider	ActivaTSP 1.8.9
Evolution 10.0	Windows W2003 Server R2 32 bits SQL server 2008 Express

16.9.2 CÓMO CREAR LAS EXTENSIONES ELASTIX

Creación de extensiones Elastix

1 Acceder a la interfaz web de administración de Elastix. El usuario/contraseña por defecto de elastix es `admin/palosanto`

2 Navegar a *PBX | PBX Configuration | Basic | Extensions* y configurar las extensiones SIP

Por ejemplo, para configurar la extensión 410, usaremos los siguientes parámetros:

Device = Generic SIP Device
User extension = 410
Display name=410
Secret = 1234

El resto de campos no son necesarios para la configuración de prueba.

Finalmente, pulsa el botón [Submit] para añadir la extensión.

3 Finalmente aplica los cambios en la configuración pulsando la barra "Apply Configuration Changes Here", situado en la parte superior del formulario.

16.9.3 CÓMO CREAR LAS COLAS ACD ELASTIX

Configuración de las colas ACD

1 Navega a *PBX | PBX Configuration | Inbound Call Control | Queues* y configura las colas ACD.
Por ejemplo, para configurar la cola 100 usaremos los siguientes parámetros:

Queue Number= "100"
Queue Name = "ACD 100"
CID Name Prefix= "100:" (Nota: debe coincidir con el 'queue number' seguido por el carácter ':')
RingStrategy = "roundrobin"
AutoFill = "Checkbox activado"

2 Finalmente, pulsa el botón [Submit Changes] para añadir las colas y no te olvides de aplicar los cambios de configuración pulsando la barra "Apply Configuration Changes Here",

situado en la parte superior del formulario

16.9.4 CÓMO CONFIGURAR UNA EXTENSIÓN TIPO ROUTE-POINT

En una configuración con campañas DBR deberá configurar una o más extensiones asterisk como “route-point” para que las llamadas puedan ser controladas por el módulo EvoRouter. Si utiliza configuración tipo “switch-based” no es necesario que administre ningún route-point.

Al configurar extensiones tipo “route-point” la configuración resultante puede ser una combinación de las siguientes:

- Cada ruta de llamadas inbound se encaminan a una extensión asterisk (Route-Point) diferente. El servidor DBR ejecutará aquella estrategia de encaminamiento cuyo DN coincida con el route-point (ej: 100)
- Varias rutas de llamadas inbound se encaminan a una misma extensión asterisk (Route-Point). El servidor DBR ejecutará aquella estrategia de encaminamiento cuyo DN coincida con el valor de la variable RDNIS de la llamada en asterisk.

Para crear una extensión asterisk que actúe como “route-point”:

1- Administre el dialplan asterisk y cree una nueva extensión, editando extensions_custom.conf
2- Configure el dialplan de la nueva extensión para que ejecute una llamada FastAGI al módulo EvoRouter del servidor.
   a. P.ej, si evorouter está escuchando en la dirección `192.168.0.177`

```
exten => 111,1,AGI(agi://192.168.0.177/EvoRouter);
```

Por ejemplo, para crear una extensión 111 tipo route-point que se conecte al módulo EvoRouter en la dirección IP 192.168.0.177:

Extensions_custom.conf

```
exten => 111,1,AGI(agi://192.168.0.177/EvoRouter);
```

Nota: Se recomienda que a continuación del comando AGI() se establezca la secuencia de pasos adecuada para tratar escenarios de fallo de enrutamiento, por ejemplo, desviar la llamada a otro destino o extensión de emergencia.

En versiones de Asterisk 1.6 o superiores es posible configurar el modo compatibilidad con versiones anteriores, que afecta a los separadores de opciones usados en AGi y FastAGI.

Puede consultarse si el modo compatibilidad está activado si en el fichero de configuración Asterisk.conf está establecido el parámetro res_agi=1.4 en la sección [compat] o dicho parámetro no existe.

En estos casos sera necesario indicar el parámerto adicional “CompatResAGIVersion=1.4” en la definición del route-point. En versiones de Elastix como la 2.0.4 18 el modo copatibilidad se encuentra activado, así que es necesario establecer este parámetro, por ejemplo:

Extensions_custom.conf

```
    exten => 111,1,AGI(agi://192.168.0.177/EvoRouter?
CompatResAGIVersion=1.4);
```

3- Asegúrese de que dispone del módulo “Misc Destinations” y que está habilitado
   a. Acceda a FreePBX, Admin, Setup y compruebe que dispone del módulo “Misc Destinations” y que está habilitado.
   b. En caso contrario instálelo mediante la opción “Check for updates online”
4- Administre una nueva entrada de tipo “misc destination” para cada extension route-point que haya creado:
   a. Acceda a FreePBX, Admin, Setup, sección “Internal Options & Configuration”, acceda al módulo “Misc Destinations”.
   b. Entre el parámetro “Description”. Ej: “Main Inbound Route Point”
   c. Edite el parámetro “dial” con el valor correspondiente a una de las extensiones route-point que anteriormente ha creado en extensions_custom.conf. Ej: “111”
   d. Submit changes, apply

Ahora podrá establecer la extensión route-point como extensión de destino en rutas de llamadas desde la propia interfaz FreePBX. Por ejemplo, para administrar una ruta de entrada:

5- Acceda a FreePBX, Admin, Setup, sección Inbound Routes
   a. Seleccione la ruta que desea administrar.
   b. Haga scroll por el formulario hasta el grupo de parámetros “Set Destination”.
   c. Seleccione la opción “Misc. Destinations” y elija la extensión route-point en el desplegable.

16.9.5 CÓMO HABILITAR LA INTERFAZ DE CONEXIÓN AMI EN ASTERISK

Ahora debemos habilitar la interfaz de comunicaciones Asterisk Management Interface (AMI) para que permita conexiones desde el servidor Evolution.

Habilitar la interfaz de comunicación asterisk management interface

1 Navegar a *PBX | Tools | File Editor*. Clicar sobre *manager.conf* para editar y cambiar los valores a

```
;
; Asterisk Call Management support
;
[general]
enabled = yes
port = 5038
bindaddr = 0.0.0.0

[admin]
secret = elastix456
#deny=
permit=0.0.0.0/0.0.0.0
read = system,call,log,verbose,command,agent,user
write = system,call,log,verbose,command,agent,user
```

```
#include manager_additional.conf
#include manager_custom.conf
```

Asegúrate de que las líneas deny y permit son correctas.

Nota: Esta configuración es válida para asterisk 1.4, que es la versión que incorpora Elastix 1.6-12. Las versiones de asterisk 1.6 o superiores requieren otros parámetros.

2 Finalmente reiniciaremos Asterisk para asegurar que todos los cambios tengan efecto:

Navegar a *System* | *Shutdown* y seleccionar la opción de *Reboot*

16.9.6 CÓMO INSTALAR ACTIVATSP (TAPI SERVICE PROVIDER)

Instalar y configurar Activa TSP en el servidor Evolution).

NOTA: Se requiere ActivaTSP 1.8.9

Descargar e instalar Activa TSP (http://activa.sourceforge.net/)

Configurar el TSP para que pueda controlar las extensiones de los agentes y las colas: inicio → Panel de control → Opciones de teléfono y modem → Opciones Avanzadas → ActivaTSP for Asterisk

Incluya las extensiones y las colas ACD que desea controlar en "Line DN". Puede utilizar una lista separada por comas, como por ejemplo DN="410-419, 100, 101".

NOTA: ActivaTSP utiliza recursos para cada DN especificado en "Line DN". Mantenga la lista de DN tan reducida como sea posible.

NOTA: No es necesario incluir las extensiones de agente que se configuren para usar el softphone integrado.

Asegúrese de que el parámetro "Line Prefix" = "AST"

Configure el usuario y password de acceso a manager. Los valores para una instalación estándar Elastix son los siguientes: user:admin, password: elastix456

Si quiere forzar un idioma para las llamadas iniciadas por CTI puede establecer el campo Orig. Variable = "CHANNEL(language)=es"

Ejemplo de parámetros ActivaTSP:

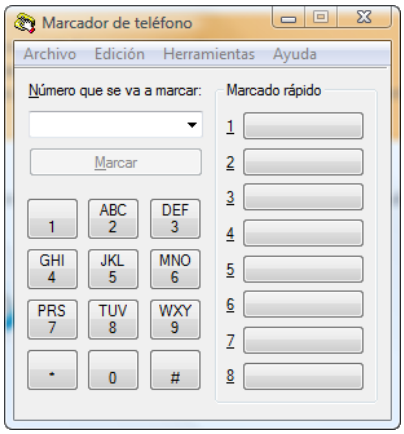
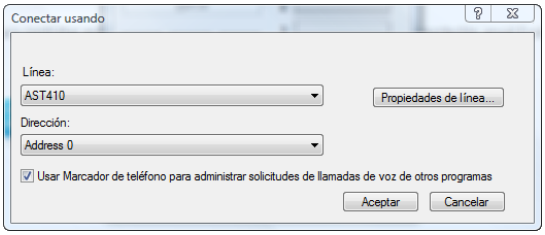
Line DN = "100-101,410-419"
Line Prefix = "AST"
Orig. Variable = "CHANNEL(language)=es"
Outgoing = "from-internal"
Agent = "from-internal"
Host IP = <*Entrar dirección IP de /ElastixTrixbox*>
Port = "5038"

User = “admin” (Nota: corresponde a la sección de usuario [admin], especificado en manager.conf)
Password = “elastix456” (Nota: corresponde al ‘secret’ especificado en manager.conf)

Tras guardar los cambios, debes reiniciar el servidor Windows 2003/2008 para asegurar que éstos tengan efecto.

16.9.7 CÓMO COMPROBAR EL CORRECTO FUNCIONAMIENTO DEL CONJUNTO ACTIVATSP / ASTERISK

Cómo comprobar el correcto funcionamiento del conjunto activatsp / asterisk

1	Desde el menú de inicio Windows, opción “ejecutar”, ejecuta la utilidad “dialer.exe”	
2	Aparecerá el diálogo “Conectar usando”, en caso contrario acceder a él mediante el menú “Herramientas | conectar usando” y seleccionar la línea correspondiente a una extensión que hayamos configurado en asterisk, p.ej: AST410	
3	En el “dialpad” telefónico marca una extensión de destino, p. ejemplo: 412	
4	Cuando pulses “marcar” debería timbrar en primer lugar la extensión de origen (410), y en cuanto la descuelgues, la llamada progresará hacia su destino (412).	

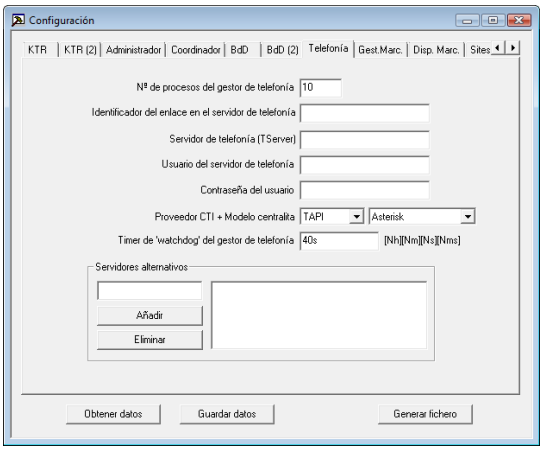
16.9.8 CÓMO CONFIGURAR EL ENLACE EVOLUTION AL SERVIDOR ASTERISK

A través de Evoadmin.exe se deberán configurar los siguientes **parámetros de telefonía:**

Parametro	Valor	Ejemplos
Identificador del enlace en el servidor de telefonía	(Vacío)	
Servidor de telefonía Tserver	(Vacío)	
Usuario y contraseña del servidor de telefonía	(Vacío)	
Proveedor CTI + Modelo centralita	TAPI/ASTERISK	Ej: TAPI/ASTERISK

Configuración de telefonía en evoadmin

Ejemplo de configuración en Evoadmin



16.9.9 CÓMO CONFIGURAR EL MÓDULO ICR DIALER DAEMON (EVODIALERSERVER)

Configuración del Servidor de Marcación con ASTERISK

1	Iniciar c:\ICR\Evolution\Server\DialerParam.exe
2	Indicar la Máquina donde está instalado el Servidor de Marcación y pulsar [Obtener Datos].

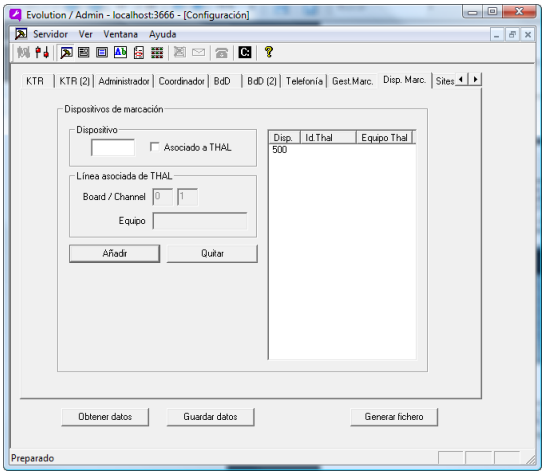
	Ej: “Maquina de Dialer”: “.” (un punto, indicando local)
3	En la pestaña DialerGlobal: > **Module** escribir el número 66 que es el correspondiente al tipo TapiAsterisk >**MainLinkID** (vacío) >**MainServerID** (vacío) >**MainLogin/MainPwd** (vacío)
4	Y pulsamos [Guardar Datos].

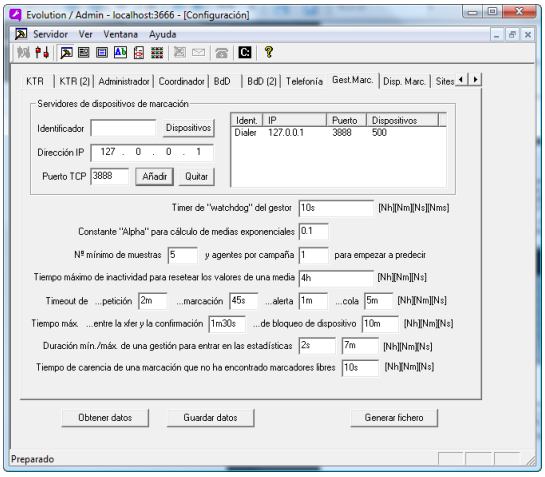
16.9.10 CÓMO ADMINISTRAR LOS DISPOSITIVOS DE MARCACIÓN EN EVOADMIN

En el caso de utilizar IP-PBX Asterisk los dichos dispositivos de marcación Evolution son dispositivos “lógicos”, y no corresponden a DN o dispositivos reales.

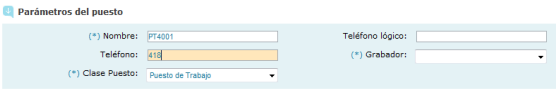
No obstante debe administrar un número suficiente y adecuado de dispositivos de marcación en Evoadmin, para soportar los procesos de marcacion.

Configuración de Dispositivos de Marcación en evoadmin

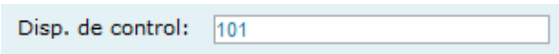
1	Ejecute evoadmin.exe, indique el *password* para operaciones restringidas, acceda al diálogo de “Configuración”, TAB “Disp. Marcador” y edite la lista de dispositivos de marcación. Pulse Guardar Datos.	

2	En el TAB “Gest. Marc.” pase a “off-line” el marcador seleccionando el identificador del “servidor de dispositivos de marcación” y pulsando el botón “Quitar”. Pulse “Dispositivos”, edite la lista de dispositivos añadiéndole todos los dispositivos correspondientes a wave ports. Una vez editados pulse “Añadir” para pasar a “on-line”. Pulse Guardar Datos.	

16.9.11 CÓMO CONFIGURAR USUARIOS Y PUESTOS EN EVOLUTION MANAGER

	Configuración Manager	
1	Administración | Puestos	Informe el número de la extensión SIP en el parámetro “teléfono” Deje vacío el “teléfono lógico” Ej: teléfono: 410 
2	Administración | Usuarios	Parámetros de usuario “login ACD” y “password ACD”: vacíos

16.9.12 CÓMO CONFIGURAR CAMPAÑAS SWITCH-BASED EN EVOLUTION MANAGER

	Configuración Manager (configuración switch-based routing)	
3	Administración | Campañas	En la sección “Routing” seleccione la opción “switch-based” Evolution determina que las llamadas *inbound* pertenecen a una campaña cuando el `calleddevice` de la llamada coincide con el DN de una estrategia DNIS asociada a la campaña. Administre una o más estrategias de tipo DNIS, asociadas a la campaña. En asterisk el valor de DNIS debe coincidir con el DN de la QUEUE ACD Asterisk que entregue las llamadas a los agentes. En la sección “Routing” administre una o más estrategias de tipo de encaminamiento ‘DNIS’, y asígnela a la campaña. Ej: Estrategia de encaminamiento tipo DNIS con DN: 100 y asociada a la campaña “atención al cliente” En la administración de campaña informe el parámetro “Disp. De control” con el QUEUE ACD Asterisk que deberá generar las llamadas predictivas/progresivas. Si la campaña no usa marcación progresiva o predictiva puede dejar este campo vacío 
4	Administración | Servicios	Configure un servicio con un ACD que coincida con el correspondiente QUEUE ACD asterisk Cuando un agente se conecte a Evolution

utilizando un Puesto de Trabajo con extensión, el servidor realizará login de esta extensión a la QUEUE ACD asterisk correspondiente al servicio.

Puede utilizar secuencias de conexión para hacer 'login' / 'logout' a colas adicionales.

Las secuencias soportadas son las siguientes:

LOGIN:
`#FEATURE=Login#QUEUE=<queue>`

LOGOUT:
`#FEATURE=Logout#QUEUE=<queue>`

Si tenemos varias campañas adicionales, podemos separar las secuencias con punto y coma. Por ejemplo, si queremos hacer login en las colas 500 y 501 haríamos:

Secuencia de conexión:
#FEATURE=Login#QUEUE=500;#FEATURE=Login#QUEUE=501
Secuencia de desconexión:
#FEATURE=Logout#QUEUE=500;#FEATURE=Logout#QUEUE=501

Recuerde que en la secuencia de conexión/desconexión no es necesario incluir la cola de la campaña que coincida con el DN del servicio.

16.9.13 CÓMO CONFIGURAR DEVELOPER SERVICE PARA SUBIR LOCUCIONES ASOCIADAS A LOS SCRIPTS DBR

Las opciones a configurar están relacionadas con el despliegue de DBR Scripts, por lo que únicamente es necesario modificar los parámetros en el caso de que se vaya a usar este tipo de estrategias.

Para configurar los parámetros tendrá que modificar el archivo web.config del directorio de instalación de Developer Service (por defecto: C:\inetpub\wwwroot\Evolution\DeveloperService). En la sección <appSettings> configure las siguientes claves:

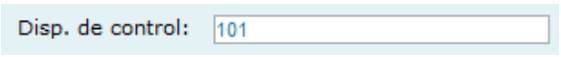
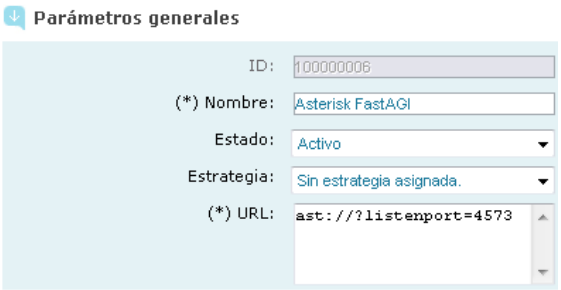
```
<!-- Parametros SFTP para audios de Script DBR -->
<add key="SFTPHost" value="scm" />
<add key="SFTPUser" value="root" />
<add key="SFTPPort" value="22" />
<add key="SFTPPassword" value="password" />
<!-- Directorio raiz donde se ubicarán las locuciones de los DBRScripts  -->
<add key="SFTPRootSounds" value="/var/lib/asterisk/sounds" />
<!-- Directorio raiz donde se gestiona Music on hold -->
```

```
<add key="SFTPRootMoh" value="/etc/asterisk/icr"/>
<!-- Directorio fuente donde se encuentran los Scripts DBR -->
<add key="DBRScripts" value="Evolution/DBRScripts"/>
<!-- Puerto AMI para hacer el reload (el host es igual que el SFTPHost) -->
<add key="AMIPort" value="5038"/>
<!-- Usuario AMI -->
<add key="AMIUser" value="evolution"/>
<!-- Password AMI -->
<add key="AMISecret" value="bomber"/>
```

Para más información ver “12 Dynamic Business Router”

16.9.14 CÓMO CONFIGURAR CAMPAÑAS DBR EN EVOLUTION MANAGER

Configuración Manager (configuración DBR)		
1	Administración | Campañas	En la sección “Routing” seleccione la opción “Evolution DBR-Server” Evolution ejecuta la estrategia de encaminamiento cuyo DN coincida con el `route-point` de la llamada. La estrategia asigna la campaña, prioridades y otros atributos. Administre una o más estrategias de tipo DBR, asociadas a la campaña. Ej: Estrategia de encaminamiento tipo DBR estático con DN: 111 y asociada a la campaña “Servicio Técnico” En la administración de campaña informe el parámetro “Disp. De control” con el DN correspondiente al `route-point` asterisk que deberá generar y tratar las llamadas predictivas de

		esa campaña.  Si la campaña no usa marcación progresiva o predictiva puede dejar esta campo vacío
2	Administración | Campañas | Conectores DBR	En la lista de campañas seleccione “Ver Conectores DBR”, y administre un nuevo conector para cada puerto FastAGI que se quiera publicar. Evolution, según el puerto (parámetro *listenport*), el contexto de los agentes (parámetro *agentscontext*) y el MusicOnHold (parámetro *moh*) especificado en la URL, atenderá las llamadas recibidas aplicando la estrategia asignada. La estrategia determina la campaña, prioridades y otros atributos. En caso de no asignar ninguna estrategia, Evolution escogerá de forma dinámica aquella cuyo DN coincida con el `route-point` de la llamada. Por defecto, el conector DBR se publica en el puerto 4573, usando el contexto para los agentes y MusicOnHold por defecto de Asterisk. El formato de configuración del conectorURL se especifica según: *Protocol://[UserInf@][[Host]:[Port]][/[Ruta][?[[ParamN]=[ValueN]]&…]]* Ej: Para publicar el conector DBR a través del puerto 4573 especifique la URL= `ast://?listenport=4573` 

16.9.15 NOTAS TÉCNICAS

Instalación y configuración de Asterisk		
1	Los nombres de las extensiones y colas controlados por Evolution deben ser numéricos. Ejemplo: “100” o “410”	Los nombres alfanuméricos (ej: “my-SIP-phone”) no están soportados
2	El dialplan de las colas ACD (ACD queue) deben forzar un Caller-ID-Name (CIDName) que comience por el número de la cola seguido por dos puntos. Ejemplo: Si la ACD queue=100, se requiere CID name prefix= "100:"	ActivaTSP utiliza este prefijo en CID-Name para identificar a qué cola pertenecen las llamadas que se ofrecen a las extensiones de los agentes.
3	La conexión LAN entre Asterisk y ActivaTSP es crítica. Por ello se recomienda que dicha conexión se realice mediante una red dedicada.	En muchos casos puede ser aconsejable dotar a ambos servidores de dos tarjetas de red (NIC), dedicando una de ellas a esta red privada Asterisk/ActivaTSP. Otras recomendaciones son las siguientes: • Establecer el parámetro de Manager.conf:-writetimeout = 500 • Configurar los siguientes parametros de los adaptadores de red: 100 Mbps, full duplex, autoneg off
4	La política de distribución de llamadas de las colas ACD (ACD queues) recomendada es rrmemory (round-robin with memory).	Otros esquemas como por ejemplo “ring all” no están soportados y pueden generar eventos erróneos.
5	En la configuración predeterminada de Elastix el número de extensión 411 coincide con una “feature-code”:	

	"Phonebook dial-by-name directory". En tal caso puedes evitar utilizar este número de extensión o, si lo prefieres, puedes cambiar el código de esta "feature-code" por otro diferente para que te permita generar la extensión=411.
6	Si no dispones de teléfonos SIP puedes utilizar soft-phones. Sugerimos que descargues e instales el soft-phone X-LITE de CounterPath (http://www.counterpath.com/x-lite.html) en los PC de agente.

17 ANEXO B: INSTALACIÓN DE MEDIASERVER PARA SOPORTE DBR

Para poder habilitar las características DBR en algunas centralitas se puede instalar un servidor complementario que denominamos MediaServer.

En general la arquitectura con MediaServer se basa en añadir un componente adicional entre la centralita y evolution. Comunicandose por un trunk de canales de voz entre la centralita y el MediaServer y por CTI entre el MediaServer y Evolution.

En concreto se puede instalar un MediaServer basado en Asterisk usando un standard del mercado como es SIP para el trunk de comunicaciones entre la centralita y el Mediaserver, y el conector DBR para Fast AGI disponible en Evolution.

17.1 CÓMO INSTALAR UN MEDIASERVER BASADO EN ELASTIX

17.1.1 CONFIGURACIÓN CERTIFICADA

La siguiente es la lista de equipos y software que se utilizó para la validación y certificación de Evolution Media Server en un entorno basado en Elastix:

Equipamiento	Software
Elastix (asterisk)	Elastix 2.3.0
IP PBX	CISCO UCM 7.1.3
Asterisk TAPI Service Provider	ActivaTSP 1.8.9
Evolution 10.2.x	Windows W2003 Server R2 32 bits SQL server 2008 Express

17.1.2 INSTALACIÓN DE ELASTIX

La opción media server puede configurarse sobre diferentes plataformas, entre las cuales ELASTIX 2.3.0.

Antes de continuar con la configuración de Media Server usted deberá instalar y realizar la configuración básica de la plataforma Elastix.

4- Descargar Elastix 2.3.0. Este software se suministra como una imagen .iso.
   a. Para más información, ver www.elastix.org
   b. NOTA: Este manual describe los pasos de instalación para Elastix-2.3.0-i386-bin-02Apr2012.iso
   c. NOTA: La instalación de ELASTIX borrará TODA la información del HD, e instalará SO Linux.
5- Si usted decide instalar el sistema en un servidor físico:
   a. Genere un CD/DVD a partir de la imagen .iso, e insértelo en el lector cd/dvd
   b. Asegúrese que el servidor está configurado para que arranque desde cd/dvd. Puede ser necesario revisar la configuración BIOS
   c. Reinicie el servidor. Con ello arrancará desde cd/dvd e iniciará el programa de instalación de ELASTIX, que le guiará paso a paso.

6- Si usted decide instalar el sistema en un servidor virtual:
   a. Copie la imagen .iso al almacén del servidor.
   b. Cree una nueva máquina virtual (VM) con configuración adecuada para Linux Redhat 5/6, y con 20GB o más de HD
   c. Vincule la unidad cd/dvd a la imagen .iso y configure la VM para que arranque desde cd/dvd
   d. Reinicie el servidor virtual. Con ello arrancará desde cd/dvd e iniciará el programa de instalación de ELASTIX, que le guiará paso a paso.
7- Una vez finalizada la instalación, compruebe que puede acceder a la interfaz web de administración de Elastix, con el usuario "admin" y el password especificado durante la instalación.

17.1.3 RECOMENDACIONES SOBRE LA CONEXIÓN LAN ENTRE EVOLUTION SERVER Y MEDIA SERVER.

La conexión LAN entre Evolution Server y Media Server es **crítica**. Por ello se recomienda que dicha conexión se realice mediante **una red dedicada**.

En muchos casos puede ser adecuado dotar a ambos servidores de dos tarjetas de red (NIC), dedicando una de ellas a esta red privada Evolution Server/Media Server.

Otras recomendaciones son las siguientes:

- Configurar los siguientes parametros de los adaptadores de red: 100 Mbps, full duplex, autoneg off
- En Media Server: Establecer el parámetro de Manager.conf: writetimeout = 500. (ver configuración, mas adelante)

17.1.4 ¿CÓMO CONFIGURAR UNA EXTENSIÓN SIP PARA PRUEBAS EN MEDIASERVER?

Configurar una extensión SIP en el servidor Media Server nos permitirá realizar llamadas de pruebas.

Para crear una extensión SIP en la plataforma *MediaServer* basada en ELASTIX::

8- Acceda a la interfaz web de administración de Elastix, con el usuario "admin"
9- Navegar a PBX | PBX Configuration | Basic | Extensions y cree las extensiones SIP:
   a. Seleccione Device = "Generic SIP Device", y pulse [Submit]
   b. Informe los siguientes parámetros: User extension (ej: "410"), Display name (ej: "410") y Secret (ej: "1234")
   c. En general, el resto de campos no son necesarios para la configuración de una extensión prueba.
   d. Finalmente, pulsa el botón [Submit] para crear la nueva extensión.
10- Una vez haya creado todas las extensiones deseadas aplique los cambios en la configuración pulsando la barra "Apply Configuration Changes Here", situado en la parte superior del formulario.

Ahora podremos instalar un softphone SIP en un PC aparte, y configurarlo para que se registre al servidor Media Server según los parámetros anteriores.

11- En un PC aparte, descargue e instale un softphone SIP.
   a. Algunas de las opciones, P.ej: Counterpath X-Lite, Zoiper o 3CX.
12- En la configuración del softphone cree un nuevo "SIP account" o edite uno existente, y configure los parámetros según los ha definido en el Media Server:
   a. Domain (ej: 192.168.0.43)
   b. User Name (ej: 618)

c. Password (ej: 618)
d. Guarde los cambios

13- Una vez configurado el softphone, realice una llamada de prueba. Para ello puede realizar una llamada a la extensión "*43", que corresponde al servicio "echo", o alternativamente realice una llamada entre extensiones.

17.1.5 ¿CÓMO REVISAR EL MODO-COMPATIBILIDAD COMPATRESAGIVERSION=1.4 DE ELASTIX?

Las versiones de Asterisk 1.6 o superiores pueden trabajar en un modo denominado "compatibilidad 1.4", que afecta a los separadores de opciones usados en AGI y FastAGI.

El valor de este parámetro "modo compatibilidad 1.4" se utilizará más adelante durante el proceso de instalación.

Por defecto, las instalaciones ELASTIX 2.3.0 tienen "compatibilidad 1.4"=SI.

Para revisar si el "modo compatibilidad 1.4" está activado edite el fichero de configuración Asterisk.conf y revise el parámetro "res_agi", en la seccion [compat]:

Asterisk.conf, sección [compat], res_agi	modo compatibilidad 1.4
res_agi no definido	SI
res_agi = 1.4	SI
res_agi = 1.6	NO

NOTA: El valor por defecto de este parámetro es res_agi=1.4

NOTA: En una plataforma ELASTIX 2.3.0 normalmente res_agi no está definido, con lo cual "modo compatibilidad 1.4"=SI

17.1.6 CÓMO CONFIGURAR UNA EXTENSIÓN TIPO ROUTE-POINT

En una configuración con campañas DBR deberá configurar una o más extensiones del Media Server asterisk como "route-points", cuyas llamadas serán controladas por el módulo EvoRouter.

Para crear extensiones que actúen como "route-point":

14- Acceder a la interfaz web de administración de Elastix.
15- Navegar a PBX | Tools y seleccionar "asterisk file editor". Edite el fichero "extensions_custom.conf" e identifique la sección correspondiente al contexto [from-internal-custom].
16- Si el "modo compatibilidad 1.4" = SI, añada las extensiones siguiendo el patrón siguiente, donde <ROUTE-POINT-EXTENSION> es el numero de extensión routepoint que queremos añadir y <EVOSERVER-IP> es la IP correspondiente al servidor Evolution.

```
exten => <ROUTE-POINT-EXTENSION>,1,AGI(agi://<EVOSERVER-IP>/EvoRouter?CompatResAGIVersion=1.4);
exten => <ROUTE-POINT-EXTENSION>,2,Hangup()
```

Por ejemplo, para añadir un nuevo route_point “1000” y si la dirección IP del servidor Evolution es 192.168.0.177 :

```
exten => 1000,1,AGI(agi://192.168.0.177/EvoRouter?CompatResAGIVersion=1.4);
exten => 1000,1,Hangup()
```

17- Finalmente, pulsa el botón [Save] y [Reload Asterisk]

NOTA: Si el “modo compatibilidad 1.4” = NO, use el siguiente patrón:

```
exten => <ROUTE-POINT-EXTENSION>,1,AGI(agi://<EVOSERVER-IP>/EvoRouter);
exten => <ROUTE-POINT-EXTENSION>,2,Hangup()
```

NOTA: Es habitual definir un rango consecutivo de extensiones.

NOTA: Se recomienda que a continuación del comando AGI() se establezca la secuencia de pasos adecuada para tratar escenarios de fallo de enrutamiento, por ejemplo, colgar la llamada o desviar la llamada a otro destino o extensión de emergencia.

17.1.7 CÓMO AGREGAR LAS EXTENSIONES ROUTE-POINT AL MÓDULO “MISC. DESTINATIONS”

18- Acceder a la interfaz web de administración de Elastix
19- Asegúrese de que dispone del módulo “Misc Destinations” y que está habilitado
    a. Acceda a PBX, PBX Configuration, Internal Options & Configuration y compruebe que dispone del módulo “Misc Destinations” y que está habilitado.
    b. En caso contrario instálelo mediante la opción “Check for updates online”
20- Administre una nueva entrada de tipo “misc destination” para cada extension route-point que haya creado:
    a. Acceda a PBX, PBX Configuration, Internal Options & Configuration acceda al módulo “Misc Destinations”.
    b. Entre el parámetro “Description”. Ej: “RoutePoint1000”
    c. Edite el parámetro “dial” con el valor correspondiente a una de las extensiones route-point que anteriormente ha creado en extensions_custom.conf. Ej: dial=“1000”
    d. Submit changes, apply

17.1.8 CÓMO CONFIGURAR UN ENLACE SIP PARA LAS LLAMADAS INBOUND (TRUNK SIP)

21- Acceder a la interfaz web de administración de Elastix
22- Acceda a PBX, PBX Configuration, Basic, Trunks.
    a. Seleccione el enlace (trunk) que desea administrar o cree uno nuevo, del tipo “SIP Trunk”.
    b. En el grupo “General Settings” informe el parámetro “Trunk Name”, ej: “sip-trunk”
    c. En el grupo “Outgoing Settings” informe el parámetro “Trunk Name”, ej: “outbound-sip-trunk”
    d. En “PEER details”:
        i. Host (ej: host=10.200.1.31)
        ii. Username (ej: username=)
        iii. Secret (ej: secret=)
        iv. Type=peer
        v. Canreinvite=yes
        vi. Dtmfmode=rfc2833
        vii. Transport=udp,tcp
        viii. Allow=all
        ix. Context=from-trunk
    e. En el grupo “Incoming Settings” informe el parámetro “USER Context”, ej: “inbound-sip-trunk”
    f. En “USER details”:
        i. Secret (ej: secret=)
        ii. Type=user
        iii. Context=from-trunk
        iv. Canreinvite=yes
        v. Transport=udp,tcp
        vi. Allow=all
    g. Submit y Apply

17.1.9 CÓMO CONFIGURAR LAS RUTAS DE LLAMADAS INBOUND

Ahora deberán crearse las rutas necesarias para encaminar las llamadas inbound hacia las diferentes extensiones route-point.

Para administrar una ruta de entrada:

23- Acceder a la interfaz web de administración de Elastix
24- Acceda a PBX, PBX Configuration, Inbound Call Control, Inbound Routes
    a. Cree una nueva ruta inbound o seleccione la ruta que desee administrar
    b. Identifique el grupo de parámetros “Set Destination”. Seleccione la opción “Misc. Destinations” y elija la extensión route-point adecuada en el desplegable.
    c. Si lo desea puede especificar mascaras de DID y/o de CallerID. En estos casos la ruta encaminará solamente las llamadas inbound cuyo DID/CID coincida con los filtros especificado. Si no indica ninguna mascara se interpretará como “any”. Ej: any DID/any CIDl
    d. Submit y Apply

17.1.10 CÓMO CONFIGURAR LAS RUTAS DE LLAMADAS OUTBOUND

Ahora deberán crearse las rutas necesarias para encaminar las llamadas outbound hacia el o los enlaces SIP correspondientes.

17.1.10.1 PARA LAS EXTENSIONES DE AGENTE

Para administrar una ruta de salida:

25- Acceder a la interfaz web de administración de Elastix
26- Acceda a PBX, PBX Configuration, Basic, Outbound Routes
    a. Cree una nueva ruta outbound o seleccione la ruta que desee administrar
    b. Identifique el grupo de parámetros “Route Settings”. Informe el parámetro “Route Name”. Ej: 4_agents
    c. Identifique el grupo de parámetros “Dial Patterns that will use this Route. Especifique un patrón adecuado para redirigir las llamadas hacia las extensiones reales de los agentes en el switch conectado al Media Server. P.ej. si las extensiones de los agentes son de la forma 4XX, donde X={0,1,..,9}, especifique match pattern=”4XX”, y deje prepend=”” y prefix=””
    d. Identifique el grupo de parámetros “Trunk Sequence for Matched Routes”, y seleccione la secuencia de enlaces a utilizar. Ej: trunk 0 =”sip-trunk”
    e. Submit y Apply

Ahora podrá establecer las diferentes extensiones route-point como extensiones de destino

17.1.10.2 PARA LAS LLAMADAS SALIENTES DE MARCADOR

Para administrar una ruta de salida:

27- Acceder a la interfaz web de administración de Elastix
28- Acceda a PBX, PBX Configuration, Basic, Outbound Routes
    a. Cree una nueva ruta outbound o seleccione la ruta que desee administrar
    b. Identifique el grupo de parámetros “Route Settings”. Informe el parámetro “Route Name”. Ej: 0_dialer
    c. Identifique el grupo de parámetros “Dial Patterns that will use this Route. Especifique un patrón adecuado para redirigir las llamadas hacia las extensiones reales de los agentes en el switch conectado al Media Server. P.ej. si la ruta de salida de su PBX es 0., donde ‘.’ significa una sequancia de dígitos de cualquiera, especifique match pattern=”0.”, y deje prepend=”” y prefix=””
    d. Identifique el grupo de parámetros “Trunk Sequence for Matched Routes”, y seleccione la secuencia de enlaces a utilizar. Ej: trunk 0 =”sip-trunk”
    e. Submit y Apply

Ahora podrá establecer las diferentes extensiones route-point como extensiones de destino

17.1.11 CÓMO COMPROBAR EL TRUNK SIP Y LAS RUTAS INBOUND/OUTBOUND

Para realizar las comprobaciones se debe haber configurado y conectado el trunk entre el MediaServer y la centralita.

Para comprobar el correcto funcionamiento del trunk SIP y de las rutas inbound/outbound, modificaremos temporalmente la ruta inbound para que dirija las llamadas a la extensión SIP /(softphone) de pruebas.

Para administrar una ruta de salida:

29- Acceder a la interfaz web de administración de Elastix
30- Acceda a PBX, PBX Configuration, Inbound Call Control, Inbound Routes
    a. Edite la ruta de entrada que desee verificar
    b. Identifique el grupo de parámetros “Set Destination”, que actualmente está seleccionada en “Misc. Destinations” y anote su configuración. Cambie la configuración a “Extensions”, y elija la extensión SIP como destino. Ej: <618> 618.
    c. Submit y Apply

De esta forma las llamadas inbound a través del Trunk SIP y la ruta seleccionada se ofrecerán la extensión SIP de pruebas.

Para verificar el funcionamiento del Trunk SIP y la ruta inbound, realice llamadas entrantes desde el PBX conectado al Media Server, con destino hacia el Trunk SIP, y compruebe que la llamada se cursa correctamente hacia la extensión SIP de pruebas.

De forma parecida, realice llamadas salientes desde la extensión SIP de pruebas con destino a una de las extensiones de los agentes, y compruebe que efectivamente la llamada saliente se cursa a través del enlace SIP hacia la extensión del PBX conectado al Media Server.

17.1.12 CÓMO HABILITAR LA INTERFAZ DE CONEXIÓN AMI

Ahora debemos habilitar la interfaz de comunicaciones Asterisk Management Interface (AMI) para que permita conexiones desde el servidor Evolution.

31- Acceder a la interfaz web de administración de Elastix
32- Navegar a PBX | Tools | Asterisk File Editor. Seleccione el archivo manager_custom.conf para su edición.
33- En este archivo cada sección especifica los permisos para un usuario diferente, p.ej la sección [admin] especifica los privilegios para un usuario “admin”. Se sugiere crear una nueva sección [evolution] a partir de los parámetros estipulados para otro usuario y ajuste los valores a:
    a. Secret (ej: “bomber”)
    b. Deny=0.0.0.0/0.0.0.0
    c. Permit=0.0.0.0/0.0.0.0
    d. Writetimeout=500
    e. Read, write (ver ejemplo)
34- Pulse [Save] y [Reload Asterisk]

Una configuración de ejemplo es la siguiente:

```
[evolution]
```

```
secret = bomber

deny=0.0.0.0/0.0.0.0

permit=0.0.0.0/0.0.0.0

writetimeout=500

read = system,call,log,verbose,command,agent,user,originate

write = system,call,log,verbose,command,agent,user,originate
```

Nota: Esta configuración es válida para asterisk 1.6, que es la versión que incorpora Elastix 2.3.0.

17.1.13 CÓMO INSTALAR ACTIVATSP (TAPI SERVICE PROVIDER)

Instalar y configurar Activa TSP en el servidor Evolution.

NOTA: Se requiere ActivaTSP 1.8.4 o superior

35- Descargar e instalar Activa TSP en el mismo servidor Windows donde se ejecutará Evolution Server
    a. Ver http://activa.sourceforge.net/
36- Configurar el TSP para que pueda controlar las extensiones route-point. Incluya también las extensiones SIP que haya definido para las pruebas:
    a. inicio → Panel de control → Opciones de teléfono y modem → Opciones Avanzadas → ActivaTSP for Asterisk
    b. Incluya en "Line DN" las extensiones route_point así como las extensiones SIP de prueba. Puede utilizar una lista separada por comas, como por ejemplo DN="1000-1019".
    c. *NOTA: ActivaTSP utiliza recursos para cada DN especificado en "Line DN". Mantenga la lista de DN tan reducida como sea posible.*
    d. *NOTA: No es necesario incluir las extensiones de agente que se configuren para usar el softphone integrado.*
    e. Asegúrese de que el parámetro "Line Prefix" = "AST"
    f. Configure el usuario y password de acceso a AMI, tal y como los ha definido previamente en el fichero manager_custom.conf de Elastix. P.ej: user="evolution", password="bomber"
37- Tras guardar los cambios, debes reiniciar el servidor Windows 2003/2008 para asegurar que éstos tengan efecto.

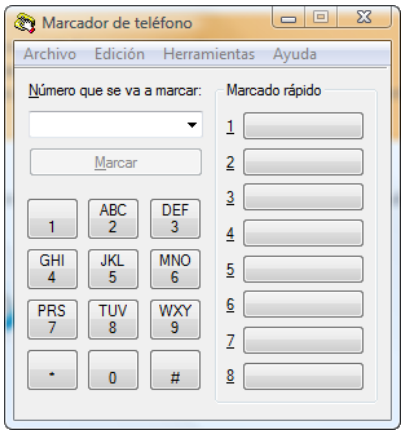
Ejemplo de parámetros ActivaTSP:

Line DN = "1000-1010,410-419"
Line Prefix = "AST"
Outgoing = "from-internal"
Agent = "from-internal"
Host IP = 192.168.0.177 <*Entrar dirección IP de /Elastix*>
Port = "5038"
User = "evolution"
Password = "bomber"

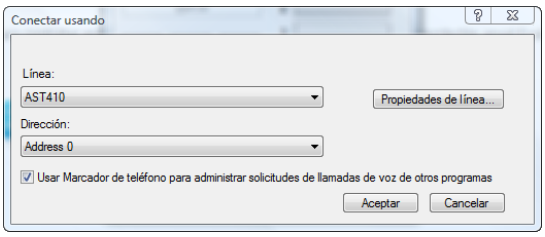
17.1.14 CÓMO COMPROBAR EL CORRECTO FUNCIONAMIENTO DEL CONJUNTO ACTIVATSP / ASTERISK

Cómo comprobar el correcto funcionamiento del conjunto activatsp / asterisk

1 Desde el menú de inicio Windows, opción “ejecutar”, ejecuta la utilidad “dialer.exe”


Marcador de teléfono
Archivo Edición Herramientas Ayuda
Número que se va a marcar:
Marcado rápido
Marcar
1 ABC 2 DEF 3
GHI 4 JKL 5 MNO 6
PRS 7 TUV 8 WXY 9
* 0 #
1 2 3 4 5 6 7 8

2 Aparecerá el diálogo “Conectar usando”, en caso contrario acceder a él mediante el menú “Herramientas | conectar usando” y seleccionar la línea correspondiente a una extensión que hayamos configurado en asterisk, p.ej: AST410



3 En el “dialpad” telefónico marca una extensión de destino, p. ejemplo: 412

4 Cuando pulses “marcar” debería timbrar en primer lugar la extensión de origen (410), y en cuanto la descuelgues, la llamada progresará hacia su destino (412).

17.1.15 CÓMO CONFIGURAR EL MODO ‘MEDIAGATEWAY’ EN EVOSERVER

Configuración del Servidor Evolution para Media Server

1 Edite el registry32, ubique la rama correspondiente a Evoserver 32 bits

2 Habilite la opción **MediaGateway** de Evoserver:

MediaGateway (DWORD) (1-Enabled, 0-Disabled)

En SO 32 bits:

HKEY_LOCAL_MACHINE\SOFTWARE\ICR\EvoServer\Coord

En SO 64 bits:

HKEY_LOCAL_MACHINE\SOFTWARE\ **WOW6432Node**\ICR\EvoServer\Coord

17.1.16 CÓMO CONFIGURAR EL MÓDULO ICR DIALER DAEMON (EVODIALERSERVER)

Configuración del Servidor de Marcación con ASTERISK

1	Iniciar c:\ICR\Evolution\Server\DialerParam.exe
2	Indicar la Máquina donde está instalado el Servidor de Marcación y pulsar [Obtener Datos]. Ej: “Maquina de Dialer”: “.” (un punto, indicando local)
3	En la pestaña DialerGlobal: > **Module** escribir el número 66 que es el correspondiente al tipo TapiAsterisk >**MainLinkID** (vacío) >**MainServerID** (vacío) >**MainLogin/MainPwd** (vacío)
4	Y pulsamos [Guardar Datos].

17.1.17 CÓMO CONFIGURAR CAMPAÑAS DBR EN EVOLUTION MANAGER

Configuración Manager (configuración DBR)

1	Administración | Campañas	En la sección “Routing” seleccione la opción “switch-based” Evolution ejecuta la estrategia de encaminamiento cuyo DN coincida con el `route-point` de la llamada. La estrategia asigna la campaña, prioridades y otros atributos. Administre una o más estrategias de tipo DBR, asociadas a la campaña. Ej: Estrategia de encaminamiento tipo DBR estático con DN: 111 y asociada a la campaña “Servicio Técnico” En la administración de campaña informe el parámetro “Disp. De control” con el DN correspondiente al `route-point` asterisk que deberá generar y tratar las llamadas predictivas de esa campaña. Si la campaña no usa marcación progresiva o predictiva puede dejar esta campo vacío
2	Administración | Campañas | Conectores DBR	En la lista de campañas seleccione “Ver Conectores DBR”, y administre un nuevo conector para cada puerto FastAGI que se quiera publicar. Evolution, según el puerto (parámetro *listenport*), el contexto de los agentes (parámetro *agentscontext*) y el MusicOnHold (parámetro *moh*) especificado en la URL, atenderá las llamadas recibidas aplicando la estrategia asignada. La

	estrategia determina la campaña, prioridades y otros atributos. En caso de no asignar ninguna estrategia, Evolution escogerá de forma dinámica aquella cuyo DN coincida con el `route-point` de la llamada. Por defecto, el conector DBR se publica en el puerto 4573, usando el contexto para los agentes y MusicOnHold por defecto de Asterisk. El formato de configuración del conectorURL se especifica según: *Protocol://[UserInf@][[Host]:[Port]][/[Ruta][?[[ParamN]=[ValueN]]&…]]* *NOTA: Para una configuración con MediaGateway debe especificar el parámetro opcional "mode=mediagateway". Y adicionalmente puede usar el parámetro "usetransfer=1" para que la entrega de la llamda al agente se realice liberando los 2 canales SIP entre la centralita y el Mediaserver.* Ej: Para publicar el conector DBR a través del puerto 4573, en modo 'mediagateway' y con el contexto from-internal especifique la URL= `ast://?listenport=4573&mode=mediagateway&agentscontext=from-internal`

17.2 CÓMO INSTALAR UN MEDIASERVER BASADO EN ASTERISK

17.2.1 CONFIGURACIÓN CERTIFICADA

La siguiente es la lista de equipos y software que se utilizó para la validación y certificación de Evolution Media Server en un entorno basado en RedHad / CentOS:

Equipamiento	Software
RedHad (asterisk)	RedHad 6.2 – Asterisk 1.8.11
IP PBX	CISCO UCM 7.1.3

Asterisk TAPI Service Provider	ActivaTSP 1.8.9
Evolution 10.2.x	Windows W2003 Server R2 32 bits SQL server 2008 Express

17.2.2 INSTALACIÓN DE ASTERISK EN REDHAD/CENTOS

Una vez se disponga de la distribución Linux RedHad o CentOS instalada se pueden seguir los siguientes pasos para instalar Asterisk.

Revisión de repositorios y "security fix"

1	Revisar que los repositorios de redhad están configurados y son accesibles. *more /etc/yum.repos.d/XXX.repo* *yum list all*	
2	Confirmar que los security fix han sido instalados *yum list updates* *#si falta alguno se puede ejecutar* *yum update*	

Instalación dependencias y desactivar SELinux

1	Comprobar que los headers del kernel actual están instalados y se corresponden. *yum install kernel-devel* *ls -la /usr/src/kernels/* *uname –a* Si no se corresponden se tiene que actualizar el kernel y reiniciar la máquina *yum update kernel* *reboot*	

2	Otras dependencias desde repositorio: *yum install make gcc gcc-c++* *yum install subversion* *yum install e2fsprogs-devel keyutils-libs-devel krb5-devel libogg libselinux-devel libsepol-devel libxml2-devel libtiff-devel gmp php-pear php-pear-DB php-gd php-mysql php-pdo kernel-devel ncurses-devel audiofile-devel libogg-devel openssl-devel mysql-devel zlib-devel perl-DateManip sendmail-cf sox*	
4	Desactivar SELinux: vi /etc/selinux/config Establecer *SELINUX=disabled*	
5	Desactivar firewall *service iptables save* *service iptables stop* *chkconfig iptables off*	

Instalación Asterisk

A continuación se listan los pasos más importantes:

INSTALACION:		
1	Descargar y instalar Asterisk: *cd /usr/src/* *wget* http://downloads.asterisk.org/pub/telephony/certified-asterisk/releases/certified-asterisk-1.8.11-cert1.tar.gz *tar -xvzf certified-asterisk-1.8.11-cert1.tar.gz* *cd certified-asterisk-1.8.11-cert1* *./configure* *make menuselect* ***(seleccionar addons mysql y cdr_mysql y mp3)***	

	(seleccionar Applictions: amd) ***(seleccionar Core Sound Packages CORE-SOUNDS-EN-ULAW)*** ***(seleccionar Music On Hold File Packages MOH-OPSOUND-ULAW)*** ***(seleccionar locuciones extra EXTRA-SOUNDS-EN-ULAW)*** *contrib/scripts/get_mp3_source.sh* *make* *make install* *make config* *make samples*	

17.2.3 RECOMENDACIONES SOBRE LA CONEXIÓN LAN ENTRE EVOLUTION SERVER Y MEDIA SERVER.

La conexión LAN entre Evolution Server y Media Server es **crítica**. Por ello se recomienda que dicha conexión se realice mediante **una red dedicada**.

En muchos casos puede ser adecuado dotar a ambos servidores de dos tarjetas de red (NIC), dedicando una de ellas a esta red privada Evolution Server/Media Server.

Otras recomendaciones son las siguientes:

- Configurar los siguientes parametros de los adaptadores de red: 100 Mbps, full duplex, autoneg off
- En Media Server: Establecer el parámetro de Manager.conf: writetimeout = 500. (ver configuración, mas adelante)

17.2.4 ¿CÓMO CONFIGURAR UNA EXTENSIÓN SIP PARA PRUEBAS EN MEDIASERVER?

Configurar una extensión SIP en el servidor Media Server nos permitirá realizar llamadas de pruebas.

Para crear una extensión SIP en la plataforma *MediaServer* basada en Asterisk:

38- Editar fichero /etc/asterisk/sip.conf
39- Añadir el siguiente contenido:

```
[618]
type=friend
host=dynamic
insecure=invite
qualify=60
nat=yes
```

```
context=default
```

40- Ejecutar el comando *asterisk –x "reload"* para aplicar la configuración.

Ahora podremos instalar un softphone SIP en un PC aparte, y configurarlo para que se registre al servidor Media Server según los parámetros anteriores.

41- En un PC aparte, descargue e instale un softphone SIP.
    a. Algunas de las opciones, P.ej: Counterpath X-Lite, Zoiper o 3CX.
42- En la configuración del softphone cree un nuevo "SIP account" o edite uno existente, y configure los parámetros según los ha definido en el Media Server:
    a. Domain (ej: 192.168.0.43)
    b. User Name (ej: 618)
    c. Password (ej: 618)
    d. Guarde los cambios
43- Una vez configurado el softphone, realice una llamada de prueba. Para ello puede realizar una llamada a la extensión "600", que corresponde al servicio "echo", o alternativamente realice una llamada entre extensiones.

17.2.5 ¿CÓMO REVISAR EL MODO-COMPATIBILIDAD COMPATRESAGIVERSION=1.4 DE ASTERISK?

Las versiones de Asterisk 1.6 o superiores pueden trabajar en un modo denominado "compatibilidad 1.4", que afecta a los separadores de opciones usados en AGI y FastAGI.

Para revisar si el "modo compatibilidad 1.4" está activado edite el fichero de configuración Asterisk.conf y revise el parámetro "res_agi", en la seccion [compat]:

Asterisk.conf, sección [compat], res_agi	modo compatibilidad 1.4
res_agi no definido	SI
res_agi = 1.4	SI
res_agi = 1.6	NO

NOTA: El valor por defecto de este parámetro es res_agi=1.4

NOTA: En una plataforma Asterisk 1.8.11 normalmente res_agi=1.6 "modo compatibilidad 1.4"=NO

17.2.6 CONFIGURACIÓN PARA QUE EL DESTINO DE CUALQUIER LLAMADA ENTRANTE POR EL TRUNK SE CONSIDERE ROUTE-POINT

En una configuración con campañas DBR deberá configurar una o varias extensión del Media Server asterisk para que distribuya las llamadas a los "route-points", cuyas llamadas serán controladas por el módulo EvoRouter. Por convenio y facilidad se configurara el dialplan para que el destino de cualquier llamada entrante se considere Route-Point.

Para crear extensiones que actúen como "route-point":

1- Edite el fichero "/etc/asterisk/extensions.conf".
2- Añada el siguiente contenido:

```
[mediagateway-trunk-in]

exten => _X.,1,AGI(agi://<EVOSERVER-IP>/EvoRouter)

exten => _X.,2,Hangup()
```

Por ejemplo, si la dirección IP del servidor Evolution es 192.168.218.67:

```
[mediagateway-trunk-in]

exten => _X.,1,AGI(agi://192.168.218.67/EvoRouter)

exten => _X.,2,Hangup()
```

3- Aplique la configuración ejecutando *asterisk –x "reload"* .

NOTA: Si el "modo compatibilidad 1.4" = SI, use el siguiente patrón:

```
exten => <ROUTE-POINT-EXTENSION>,1,AGI(agi://<EVOSERVER-IP>/EvoRouter?CompatResAGIVersion=1.4);

exten => <ROUTE-POINT-EXTENSION>,2,Hangup()
```

NOTA: Es habitual definir un rango consecutivo de extensiones.

NOTA: Se recomienda que a continuación del comando AGI() se establezca la secuencia de pasos adecuada para tratar escenarios de fallo de enrutamiento, por ejemplo, colgar la llamada o desviar la llamada a otro destino o extensión de emergencia.

17.2.7 CÓMO CONFIGURAR UN ENLACE SIP PARA LAS LLAMADAS INBOUND (TRUNK SIP)

4- Edite el fichero /etc/Asterisk/sip.conf
5- Añada el siguiente contenido:

```
[CiscoTrunkSip]

type=friend
```

```
context=mediagateway-trunk-in

host=192.168.218.10

disallow=all

allow=ulaw

allow=alaw

nat=no

canreinvite=yes

qualify=yes

dtmfmode=rfc2833
```

6- Ejecutar el comando *asterisk –x "reload"* para aplicar la configuración.

17.2.8 CÓMO CONFIGURAR LAS RUTAS DE LLAMADAS "OUTBOUND"

Ahora deberán crearse las rutas necesarias para encaminar las llamadas outbound hacia la PBX, gracias a estas rutas las llamadas encoladas podrán ser entregadas a los agentes y se podrán emitir llamadas salientes por ejemplo para marcación automática.

1- Editar el fichero /etc/asterisk/extensions.conf
2- Añada el siguiente contenido:

```
[mediagateway-trunk-out]

exten => _X.,1,Dial(SIP/CiscoTrunkSip/${EXTEN})

exten => _X.,n,Hangup()
```

3- Aplique la configuración ejecutando *asterisk –x "reload"* .

17.2.9 CÓMO COMPROBAR EL TRUNK SIP Y LAS RUTAS INBOUND/OUTBOUND

Para realizar las comprobaciones se debe haber configurado y conectado el trunk entre el MediaServer y la centralita.

Para comprobar el correcto funcionamiento del trunk SIP y de las rutas inbound/outbound, modificaremos temporalmente la ruta inbound para que dirija las llamadas a la extensión SIP /(softphone) de pruebas.

Podemos realizar esta operación editando la sección correspondiente [mediagateway-trunk-in] en el fichero /etc/asterisk/extensions.conf :

```
[mediagateway-trunk-in]

exten => _X.,1,Dial(SIP/618)

;exten => _X.,1,AGI(agi://192.168.218.67/EvoRouter)

exten => _X.,2,Hangup()
```

Aplique la configuración ejecutando *asterisk –x "reload"* .

De esta forma las llamadas inbound a través del Trunk SIP y la ruta seleccionada se ofrecerán la extensión SIP de pruebas.

Para verificar el funcionamiento del Trunk SIP y la ruta inbound, realice llamadas entrantes desde el PBX conectado al Media Server, con destino hacia el Trunk SIP, y compruebe que la llamada se cursa correctamente hacia la extensión SIP de pruebas.

Una vez realizada la verificación vuelva a dejar el fichero /etc/asterisk/extensions.conf para que las llamadas entrantes sean controladas por Evolution:

```
[mediagateway-trunk-in]

exten => _X.,1,AGI(agi://192.168.218.67/EvoRouter)

exten => _X.,2,Hangup()
```

Aplique la configuración ejecutando *asterisk –x "reload"* .

Realice llamadas salientes desde la extensión SIP de pruebas con destino a una de las extensiones de los agentes, y compruebe que efectivamente la llamada saliente se cursa a través del enlace SIP hacia la extensión del PBX conectado al Media Server.

Para permitir que la extensión editar la sección [618] para que uso el contexto "mediagateway-trunk-out":

```
[618]

type=friend

host=dynamic

insecure=invite

qualify=60

nat=yes

context=mediagateway-trunk-out
```

Aplique la configuración ejecutando *asterisk –x "reload"* .

17.2.10 CÓMO HABILITAR LA INTERFAZ DE CONEXIÓN AMI

Ahora debemos habilitar la interfaz de comunicaciones Asterisk Management Interface (AMI) para que permita conexiones desde el servidor Evolution.

1- Editar el fichero /etc/asterisk/manager.conf.
2- Establecer el parámetro "enabled = yes" en la sección [general].
3- En este archivo especificar los permisos para un usuario diferente, p.ej la sección [admin] especifica los privilegios para un usuario "admin". Se sugiere crear una nueva sección [evolution] a partir de los parámetros estipulados para otro usuario y ajuste los valores a:
    a. Secret (ej: "bomber")

b. Deny=0.0.0.0/0.0.0.0
c. Permit=0.0.0.0/0.0.0.0
d. Writetimeout=500
e. Read, write (ver ejemplo)

4- Aplique la configuración ejecutando *asterisk –x "reload"*

Una configuración de ejemplo es la siguiente:

```
[evolution]

secret = bomber

deny=0.0.0.0/0.0.0.0

permit=0.0.0.0/0.0.0.0

writetimeout=500

read = system,call,log,verbose,command,agent,user,originate

write = system,call,log,verbose,command,agent,user,originate
```

Nota: Esta configuración es válida para asterisk 1.8.11

17.2.11 CÓMO INSTALAR ACTIVATSP (TAPI SERVICE PROVIDER)

Instalar y configurar Activa TSP en el servidor Evolution.

NOTA: Se requiere ActivaTSP 1.8.9 o superior

1- Descargar e instalar Activa TSP en el mismo servidor Windows donde se ejecutará Evolution Server
   f. Ver http://activa.sourceforge.net/
2- Configurar el TSP para que pueda controlar las extensiones route-point. Incluya también las extensiones SIP que haya definido para las pruebas:
   g. inicio → Panel de control → Opciones de teléfono y modem → Opciones Avanzadas → ActivaTSP for Asterisk
   h. Incluya en "Line DN" las extensiones route_point así como las extensiones SIP de prueba. Puede utilizar una lista separada por comas, como por ejemplo DN="1000-1019".
   i. *NOTA: ActivaTSP utiliza recursos para cada DN especificado en "Line DN". Mantenga la lista de DN tan reducida como sea posible.*
   j. *NOTA: No es necesario incluir las extensiones de agente que se configuren para usar el softphone integrado.*
   k. Asegúrese de que el parámetro "Line Prefix" = "AST"
   l. Configure el usuario y password de acceso a AMI, tal y como los ha definido previamente en el fichero manager.conf. P.ej: user="evolution", password="bomber"
   m. Configure el Outgoing Context con el contexto que encamina las llamadas hacia el trunk con cisco para permitir realizar llamadas salientes al módulo marcador, en nuestro ejemplo mediagateway-trunk-out.
3- Tras guardar los cambios, debes reiniciar el servidor Windows 2003/2008 para asegurar que éstos tengan efecto.

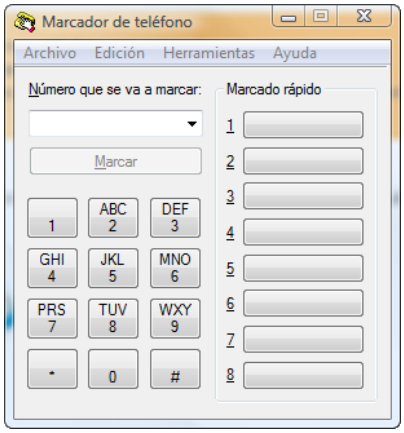
Ejemplo de parámetros ActivaTSP:

Line DN = “1000-1010,410-419”
Line Prefix = “AST”
Outgoing = “mediagateway-trunk-out”
Agent = “from-internal”
Host IP = 192.168.0.177 <*Entrar dirección IP de /Asterisk*>
Port = “5038”
User = “evolution”
Password = “bomber”

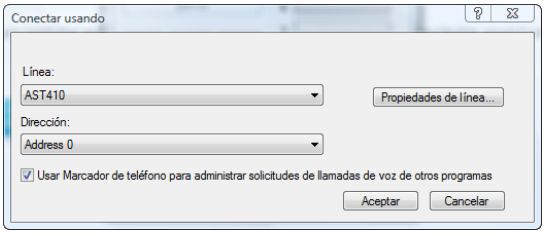
17.2.12 CÓMO COMPROBAR EL CORRECTO FUNCIONAMIENTO DEL CONJUNTO ACTIVATSP / ASTERISK

Cómo comprobar el correcto funcionamiento del conjunto activatsp / asterisk

1 Desde el menú de inicio Windows, opción “ejecutar”, ejecuta la utilidad “dialer.exe”


Marcador de teléfono
Archivo Edición Herramientas Ayuda
Número que se va a marcar:
Marcado rápido
Marcar
1 ABC 2 DEF 3
GHI 4 JKL 5 MNO 6
PRS 7 TUV 8 WXY 9
* 0 #
1 2 3 4 5 6 7 8

2 Aparecerá el diálogo “Conectar usando”, en caso contrario acceder a él mediante el menú “Herramientas | conectar usando” y seleccionar la línea correspondiente a una extensión que hayamos configurado en asterisk, p.ej: AST410



3 En el “dialpad” telefónico marca una extensión de destino, p. ejemplo: 412

4 Cuando pulses “marcar” debería timbrar en primer lugar la extensión de origen (410), y en cuanto la descuelgues, la llamada progresará hacia su destino (412).

17.2.13 CÓMO CONFIGURAR EL MODO 'MEDIAGATEWAY' EN EVOSERVER

Configuración del Servidor Evolution para Media Server	
1	Edite el registry32, ubique la rama correspondiente a Evoserver 32 bits
2	Habilite la opción **MediaGateway** de Evoserver: **MediaGateway** (DWORD) (1-Enabled, 0-Disabled) En SO 32 bits: HKEY_LOCAL_MACHINE\SOFTWARE\ICR\EvoServer\Coord En SO 64 bits: HKEY_LOCAL_MACHINE\SOFTWARE\ **WOW6432Node**\ICR\EvoServer\Coord

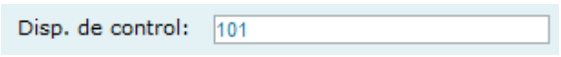
17.2.14 CÓMO CONFIGURAR EL MÓDULO ICR DIALER DAEMON (EVODIALERSERVER)

Configuración del Servidor de Marcación con ASTERISK	
1	Iniciar c:\ICR\Evolution\Server\DialerParam.exe
2	Indicar la Máquina donde está instalado el Servidor de Marcación y pulsar [Obtener Datos]. Ej: "Maquina de Dialer": "." (un punto, indicando local)
3	En la pestaña DialerGlobal: > **Module** escribir el número 66 que es el correspondiente al tipo TapiAsterisk >**MainLinkID** (vacío)

	>**MainServerID** (vacío) >**MainLogin/MainPwd** (vacío)
4	Y pulsamos [Guardar Datos].

17.2.15 CÓMO CONFIGURAR CAMPAÑAS DBR EN EVOLUTION MANAGER

Configuración Manager (configuración DBR)		
1	Administración | Campañas	En la sección “Routing” seleccione la opción “Evolution DBR-Server” Evolution ejecuta la estrategia de encaminamiento cuyo DN coincida con el `route-point` de la llamada. La estrategia asigna la campaña, prioridades y otros atributos. Administre una o más estrategias de tipo DBR, asociadas a la campaña. Ej: Estrategia de encaminamiento tipo DBR estático con DN: 111 y asociada a la campaña “Servicio Técnico” En la administración de campaña informe el parámetro “Disp. De control” con el DN correspondiente al `route-point` asterisk que deberá generar y tratar las llamadas predictivas de

		esa campaña.  Si la campaña no usa marcación progresiva o predictiva puede dejar esta campo vacío
2	Administración | Campañas | Conectores DBR	En la lista de campañas seleccione “Ver Conectores DBR”, y administre un nuevo conector para cada puerto FastAGI que se quiera publicar. Evolution, según el puerto (parámetro *listenport*), el contexto de los agentes (parámetro *agentscontext*) y el MusicOnHold (parámetro *moh*) especificado en la URL, atenderá las llamadas recibidas aplicando la estrategia asignada. La estrategia determina la campaña, prioridades y otros atributos. En caso de no asignar ninguna estrategia, Evolution escogerá de forma dinámica aquella cuyo DN coincida con el `route-point` de la llamada. Por defecto, el conector DBR se publica en el puerto 4573, usando el contexto para los agentes y MusicOnHold por defecto de Asterisk. El formato de configuración del conectorURL se especifica según: *Protocol://[UserInf@][[Host]:[Port]][/[Ruta][?[[ParamN]=[ValueN]]&…]]* *NOTA: Para una configuración con MediaGateway debe especificar el parámetro opcional “mode=mediagateway”. Y adicionalmente puede usar el parámetro “usetransfer=1” para que la entrega de la llamda al agente se realice liberando los 2 canales SIP entre la centralita y el Mediaserver.* Ej: Para publicar el conector DBR a través del puerto 4573, en modo ‘mediagateway’ y con el contexto mediagatway-trunk-out especifique la URL= `ast://?listenport=4573&mode=mediagateway&agentscontext=mediagateway-trunk-out`

17.2.16 CÓMO CONFIGURAR DEVELOPER SERVICE PARA QUE DESPLIEGUE LOS AUDIOS EN EL MEDIA SERVER

Para que los recursos de audio puedan ser desplegados en el Media Server hay que configurar el servicio de despliegue. Para configurarlo hay que editar el fichero C:\Inetpub\wwwroot\Evolution\DeveloperService\Web.config y configurar los parámetros correspondientes a la conexión SFTP y AMI:

1- SFTPHost: Nombre de host o IP del Media Server.
2- SFTPUser: Nombre de un usuario con privilegios para copiar archivos en directorios de sonido y editar configuraciones bajo los directorios indicados por los parámetros SFTPRootSounds y SFTPRootMoh.
3- SFTPPort: Puerto para la conexión SFTP.
4- SFTPPassword: Password para la conexión SFTP.
5- AMIUser: Usuario para la conexión AMI.
6- AMISecret: Secreto para la conexión AMI.
7- AMIPort: Puerto para la conexión AMI.

Por ejemplo:

```
<!-- Parametros SFTP para audios de Script DBR -->
<add key="SFTPHost" value="192.168.218.230" />
<add key="SFTPUser" value="root" />
<add key="SFTPPort" value="22" />
<add key="SFTPPassword" value="1234" />
<!-- Directorio raiz donde se ubicarán las locuciones de los DBRScripts  -->
<add key="SFTPRootSounds" value="/var/lib/asterisk/sounds" />
<!-- Directorio raiz donde se gestiona Music on hold -->
<add key="SFTPRootMoh" value="/etc/asterisk"/>
<!-- Directorio fuente donde se encuentran los Scripts DBR -->
<add key="DBRScripts" value="Evolution/DBRScripts"/>
<!-- Puerto AMI para hacer el reload (el host es igual que el SFTPHost) -->
<add key="AMIPort" value="5038"/>
<!-- Usuario AMI -->
<add key="AMIUser" value="evolution"/>
<!-- Password AMI -->
<add key="AMISecret" value="bomber"/>
```

Adicionalmente, para que la Music On Hold se despliegue correctamente se requiere añadir un "include" al fichero de configuración de Music On Hold generado por Developer Service. Así que en una instalación por defecto se debería añadir la siguiente línea al final del archivo de configuración /etc/asterisk/musiconhold.conf:

```
#include icr/icr.moh.conf
```

17.3 CONFIGURACIÓN ESPECÍFICA PARA CISCO COMMUNICATIONS MANAGER CM/UCM

Recomendado con TAPI CISCO.

Evolution soporta los siguientes tipos de campaña con CISCO CM:

- Inbound DBR
- Outbound VP
- Outbound predictivo/progresivo DBR

Para los modos Inbound DBR y Outbound predictivo/progresivo DBR con MediaSever, Evolution hace uso del conector CTI Fast Agi para Asterisk.

17.3.1 CONFIGURACIÓN CERTIFICADA

La siguiente es la lista de equipos y software que se utilizó para la validación y certificación de Evolution en un entorno CISCO CM:

Equipamiento	Software
Cisco Unified Communications Manager	Release 7.1.3
IP softphone	CISCO IP Communicator v7.0.3.3
Cisco TSP for Windows32	Version 7.1(3.4)
Evolution 10.2.1	Windows W2003 Server R2 32 bits SQL server 2008 Express

17.3.2 CÓMO CONFIGURAR LOS ELEMENTOS CTI ESPECÍFICOS PARA CISCO

Es recomendable configurar los elementos CTI según el capítulo: 16.5 CISCO Communications Manager CM/UCM.

Si prefiere solo configurar los elementos estrictamente necesarios para la configuración Cisco basada en MediaServer puede basarse en los siguientes capítulos:

- 16.5.2 Cómo administrar un usuario Cisco para Evolution.

- 16.5.3 Cómo asociar las líneas de los teléfonos al usuario Evolution.
- 16.5.7 Cómo instalar los componentes CiscoTSP y Cisco Wave Driver.
- 16.5.8 Cómo comprobar el correcto funcionamiento de CiscoTSP.
- 16.5.9 Cómo configurar el enlace Evolution al CISCO TAPI.
- 16.5.12 Cómo configurar usuarios y puestos en Evolution Manager.

17.3.3 CONFIGURAR TRUNK SIP EN CISCO

Preparar perfil de seguridad de Trunk SIP compatible con Media Server:

1- Acceder a la interfaz web de Cisco Unified CM Administration.
2- Ir a “System Security”>”Sip Trunk Security Profile”
3- Copiar o modificar el perfil Non Secure Sip Trunk Profile.
4- Establecer el campo Outgoing Transport = UDP.

Para configurar el trunk sip en Cisco:

1- Acceder a la interfaz web de Cisco Unified CM Administration.
2- Acceder a la pantalla device>trunk y pulsar en “add new”.
3- Para el “Trunk Information” rellenar los campos:
    n. Trunk Type = SIP Trunk
    o. Device Protocol = SIP
    p. Pulsar “next”.
4- En el panel “Device Information” rellenar los campos:
    q. Device Name = MediaGatewayAsterisk
    r. Device Pool = Default
    s. Marcar la opción Media Termination Point Required.
5- En el panel “SIP Information” rellenar los campos:
    t. Destination Addres = <IP-MediaServer>
    u. SIP Trunk Security Profile = “Non Secure SIP Trunk Profile”
    (se debe usar el peril de seguridad configurado con Outgoing Transport = UDP)
    v. SIP Profile = “Standard SIP Profile”
    w. DTMF Signaling Mode = RFC2833
6- Pulsar “save” y “Apply Config”.

Por ejemplo para que se puedan dirigir las llamadas desde el CISCO al MediaServer se puede usar un RoutePattern 0!, así todas las llamadas a números que empiezan por 0 se dirigirán hacia el trunk.

1- Acceder a la pantalla “Call Routing>Route Hund>Route Pattern”
2- Pulse en “add new” y rellene los sigientes parametros.
    a. Route Pattern = 0!
    b. Gateway/Router List = MediaGatewayAsterisk.
3- Pulsar “save” y “Apply Config”.

El administrador de Cisco debe decidir cuál es el mejor método para dirigir las llamadas hacia el MediaServer.

17.4 CONFIGURACIÓN PARA AVAYA AURA COMMUNICATIONS MANAGER

Puede interconectarse un servidor Evolutiion SIP CallManager / Evolution Media Server con AVAYA AURA Communications Manager mediante TRUNK-SIP.

17.4.1 CONFIGURAR TRUNK SIP EN AVAYA CM

Sugerimos seguir los procedimientos definidos en “Configuring Avaya Communication Manager and Avaya SIP Enablement Services for SIP Trunks with Asterisk Business Edition PBX – Issue 1.0” de AVAYA Inc.

17.4.2 CONFIGURAR SIP CALL MANAGER

Siga las instrucciones genéricas de configuración Evolution SIP Call Manager/Media Server:

- “17.2 Cómo instalar un MediaServer basado en Asterisk”
- “17.2.7Cómo configurar un enlace SIP para las llamadas inbound (trunk SIP)”

Si en AVAYA se usa transporte TCP en lugar de UDP, entonces se deberá habilitar SIP sobre TCP en el SipCallManager. Para ello:

1- Edite el fichero /etc/asterisk/sip_general_custom.conf:

```
tcpenable=yes

tcpbindaddr=0.0.0.0
```

2- Edite la configuración del TRUNK:

En la configuración del trunk hay que añadir el parámetro transport=tcp en la caja de texto correspondiente a “PEER Details”:

```
host=192.168.0.X

dtmfmode=rfc2833

context=from-pstn

qualify=yes

type=friend

insecure=port,invite

transport=tcp
```

18 ANEXO C: CONFIGURACIÓN DE CONECTORES DBR NO INTERACTIVOS

Evolution server además del canal telefónico soporta otros canales.

Es posible integrar otros canales, consultar el manual de integración.

18.1 CONECTOR DBR POP3/POP3S

18.1.1 PREREQUISITOS

Disponer de una cuenta pop3/pop3s que se quiera atender con el motor DBR de Evolution.

18.1.1 CÓMO CONFIGURAR EL CONECTOR POP3/POP3S EN EVOLUTION MANAGER

	Configuración Manager (configuración DBR)	
1	Administración | Campañas | Estrategias	En la lista de campañas seleccione “Ver Estrategias”, y administre una o más estrategias de encaminamiento. Ej: Estrategia de encaminamiento de tipo “DBR estático” que ofrece las llamadas a la cola de la campaña “Servicio técnico DBR e-mail”
2	Administración | Campañas | Conectores DBR	En la lista de campañas seleccione “Ver Conectores DBR”, y administre un nuevo conector para cada cuenta POP3/POP3S. Evolution monitorizará el buzón de correo especificado en la URL, y tratará los mails recibidos aplicando la estrategia asignada. La estrategia

		determina la campaña, prioridades y otros atributos. Evolution ejecuta la estrategia de encaminamiento especificada en el conector o aquella cuyo DN coincida con UserName del buzón de correo especificado. El formato de configuración del conectorURL se especifica según: *Protocol://[UserInf@][[Host]:[Port]][/[Ruta][?[[ParamN]=[ValueN]]&…]]* Ej: Para controlar el buzón de correo soporte@test.com especifique URL=`pop3://soporte:123!@test.com:110` o URL=`pop3s://soporte:123!@test.com:995`
3	Administración | Campañas	En la sección “Routing” seleccione la opción “Evolution DBR-Server” Administre una o más estrategias de tipo DBR, asociándolas a la campaña.

En determinados casos puede ser necesario codificar alguna de las partes que forman la URL de definición del conector, para evitar que contengan caracteres inadecuados. Por ejemplo, algunos servidores email POP3 requieren especificar un dominio en el nombre de usuario:

```
usuario@dominio.com
```

En estos casos, cuando se escribe la URL correspondiente a un conector email POP3 DBR, el caracter @ deberá codificarse según las normas estandar de URLs.

Ver “18.5 Como codificar caracteres especiales en las definiciones de conectores (URL)”

18.2 CONECTOR DBR EMAIL IMAP(S)

18.2.1 PREREQUISITOS

Disponer de una cuenta email en un servidor que soporte protocolo IMAP o IMAP/S.

18.2.2 PARÁMETROS IMAP

El conector permite configurar los siguientes parámetros:

parámetro	descripción	default
Servidor	Dirección TCP/IP del servidor	
Puerto	Puerto TCP/IP Ej: 143 (IMAP), 993 (IMAP/S)	
Cuenta de usuario	Cuenta del usuario IMAP Ej: demo01	
Contraseña	Contraseña de la cuenta IMAP	
SSL	Usa SSL para encriptar las comunicaciones IMAP? (true/false)	
treatOnlyUnseen	Solamente trata los emails con la marca 'unseen' (no leídos) (true/false)	true
deleteOnTreated	¿Borra los mensajes una vez tratados? (true/false)	false
markAsSeenOnTreated	¿Marca los mensajes como tratados? (true/false)	true
fromFolder	Carpeta de la que leerá los emails Ej: fromFolder = junk e-mail	Por defecto se leen de la carpeta estándar "INBOX"
moveToFolderOnTreated	Carpeta a la que se moverán los mensajes tratados Ej: moveToFolderOnTreated = tratados	

El formato de configuración del conector se especifica según un formato tipo URL:

Protocol://[UserInf@][[Host]:[Port]]/[Ruta][?[[ParamN]=[ValueN]]&…]]

Ejemplo:

- Servidor mail.servere.com
- Usuario/contraseña: `demo01 / demo123!`
- DeleteOnTreated = true
- TreatOnlyUnseen = yes

```
imaps://demo01:demo123!@mail.server.com?deleteOnTreated=true&treatOnlyUnseen=yes
```

18.2.3 CÓMO CONFIGURAR EL CONECTOR IMAP(S) EN EVOLUTION MANAGER

	Configuración Manager (configuración DBR)	
1	Administración | Campañas | Estrategias	En la lista de campañas seleccione "Ver Estrategias", y administre una o más estrategias de encaminamiento. Ej: Estrategia de encaminamiento de tipo "DBR estático" que ofrece las llamadas a la cola de la campaña "Servicio técnico DBR e-mail"
2	Administración | Campañas | Conectores DBR	En la lista de campañas seleccione "Ver Conectores DBR", y administre un nuevo conector para cada cuenta IMAP. Evolution monitorizará el buzón de correo especificado en la URL, y tratará los mails recibidos aplicando la estrategia asignada. La estrategia determina la campaña, prioridades y otros

		atributos. Evolution ejecuta la estrategia de encaminamiento especificada en el conector o aquella cuyo DN coincida con UserName del buzón de correo especificado. Ej: Para controlar el buzón de correo soporte@test.com, con password `pwd123!,` mediante IMAP/S, especifique: `imaps://soporte:pwd123!@test.com`
3	Administración | Campañas	En la sección “Routing” seleccione la opción “Evolution DBR-Server” Administre una o más estrategias de tipo DBR, asociándolas a la campaña.

En determinados casos puede ser necesario codificar alguna de las partes que forman la URL de definición del conector, para evitar que contengan caracteres inadecuados.

Ver “18.5 Como codificar caracteres especiales en las definiciones de conectores (URL)”

18.3 CONECTOR DBR WEBSERVICE API

18.3.1 CÓMO CONFIGURAR EL CONECTOR WEBSERVICE API EN EVOLUTION MANAGER

Evolution puede publicar un servicio web (WebService API) que implementa los métodos públicos necesarios para permitir a aplicaciones externas la posibilidad de encolar, obtener información y desencolar interacciones no interactivas en EvoServer.

Configuración Manager (configuración DBR)		
1	Administración | Campañas | Estrategias	En la lista de campañas seleccione “Ver Estrategias”, y administre una o más estrategias de encaminamiento. Ej: Estrategia de encaminamiento de tipo “DBR estático” que ofrece las llamadas a la cola de la campaña “Servicio técnico DBR”
2	Administración | Campañas | Conectores DBR	En la lista de campañas seleccione “Ver Conectores DBR”, y administre un nuevo conector de tipo WebService API (WSAPI). Evolution publicará el WebService API según el puerto (parámetro *listenport*) y el nombre del servicio (parámetro *servicename*) especificado en la URL (Nota: sólo es posible publicar un único WebService API). Por defecto, el WebService se publica en *http://[MACHINE_NAME]:3664/EvoRouterAPI*.

		Este WebService resolverá las peticiones que reciba aplicando la estrategia asignada al conector DBR. La estrategia determina la campaña, prioridades y otros atributos. En caso de no asignar ninguna estrategia, Evolution escogerá de forma dinámica aquella cuyo DN coincida con el RoutePoint indicado en la petición de QueueDocument al WebService. El formato de configuración del conectorURL se especifica según: *Protocol://[UserInf@][[Host]:[Port]][/[Ruta][?[[ParamN]=[ValueN]]&…]]* Ej: Para publicar en el puerto *3664* con el nombre de servicio *`EvoRouterAPI`* especifique la URL= `wsapi://?listenport=3664&servicename=EvoRouterAPI`
3	Administración | Campañas	En la sección “Routing” seleccione la opción “Evolution DBR-Server” Administre una o más estrategias de tipo DBR, asociándolas a la campaña.

En determinados casos puede ser necesario codificar alguna de las partes que forman la URL que define el conector, para evitar que contengan caracteres inadecuados.

Ver “18.5 Como codificar caracteres especiales en las definiciones de conectores (URL)”

18.4 CONECTOR DBR TWITTER

Evolution puede monitorizar cuentas de Twitter con el objetivo de encolar en EvoServer los tweets que cumplan con los criterios configurados en el conector DBR.

Evolution permite el tratamiento de tweets originados por Mensajes directos (DM) y Menciones a una cuenta Twitter monitorizada. También permite tratar todos los tweets resultantes de una búsqueda en Twitter.

18.4.1 PREREQUISITOS

Disponer de una cuenta de Twitter que se quiera atender con el motor DBR de Evolution, vinculada a una aplicación Twitter con derechos de acceso de lectura/escritura/mensajes directos.

Para crear una aplicación Twitter se debe acceder a https://dev.twitter.com identificándose con la cuenta de Twitter a monitorizar y acceder al apartado de 'My applications' para crear una aplicación.

Una vez creada la aplicación, habrá que permitirle el acceso de lectura, escritura y mensajes directos y crear el token de acceso para la autenticación del conector DBR.

Una vez realizado este proceso, deberemos disponer del *ConsumerKey*, el *ConsumerSecret*, el *AccessToken* y el *AccessTokenSecret* de la aplicación creada para la cuenta de Twitter a monitorizar.

Estos parámetros de autenticación permitirán al conector DBR acceder a la cuenta de Twitter que se quiere monitorizar.

18.4.2 CÓMO CONFIGURAR UN CONECTOR TWITTER EN EVOLUTION MANAGER

Configuración Manager (configuración DBR)		
1	Administración | Campañas | Estrategias	En la lista de campañas seleccione "Ver Estrategias", y administre una o más estrategias de encaminamiento. Ej: Estrategia de encaminamiento de tipo "DBR estático" que ofrece las llamadas a la cola de la campaña "Atención al cliente Twitter"

2	Administración | Campañas | Conectores DBR	Evolution monitorizará la cuenta de Twitter especificada en la URL, y tratará los tweets recibidos aplicando la estrategia asignada. La estrategia determina la campaña, prioridades y otros atributos. Evolution ejecuta la estrategia de encaminamiento especificada en el conector o aquella cuyo DN coincida con UserName de la cuenta de Twitter especificada. El formato de configuración del conectorURL se especifica según el estandar: *Protocol:///[UserInf@][[Host]:[Port]][/[Ruta][?[[ParamN]=[ValueN]]&…]]* El protocolo para un conector DBR Twitter es: ***twitter***. Los parámetros de configuración de un conector son: • **dm**: indica si se han de tratar los mensajes directos [true| false]. • **mentions**: indica si se han de tratar las menciones al usuario [true| false]. • **search**: indica la sentencia de búsqueda según el formato estandar de búsqueda de Twitter (https://twitter.com/#!/search-advanced). • **sincedate**: indica la fecha a partir de la cual se han de aceptar los tweets [dd/mm/yyyy]. • **tag**: permite incorporar la propiedad tag al documento. Esta propiedad podrá ser accedida desde la aplicación de agente para poder identificar el conector. • **consumerkey**: clave de la aplicación obtenida desde dev.twitter.com. • **consumersecret**: secret de la aplicación obtenida desde dev.twitter.com.

		• **accesstoken**: clave del permiso obtenida desde dev.twitter.com. • **accesstokensecret**: secret del permiso obtenida desde dev.twitter.com. Ej: Para monitorizar los mensaje directos, las menciones y los tweets en español que contienen la palabra clave "CallCenter" especifique: *twitter://?dm=true&mentions=true&search=CallCenter lang:es&consumerkey=lksjcBCOu4udVM2mNkk&consumersecret=uNcikQ9eVk4q6699R5zIW7aDI&accesstoken=426607120-QDVeBXId7mA8KF6CTQ83UGaYqI&accesstokensecret=GuifO23ArhA9GFFhbw9uCKdQctWX6ez*
3	Administración | Campañas	En la sección "Routing" seleccione la opción "Evolution DBR-Server" Administre una o más estrategias de tipo DBR, asociándolas a la campaña.

En determinados casos puede ser necesario codificar alguna de las partes que forman la URL que define el conector, para evitar que contengan caracteres inadecuados.

Ver "18.5 Como codificar caracteres especiales en las definiciones de conectores (URL)"

18.4.3 NOTAS TÉCNICAS

Comportamiento de un conector DBR Twitter		
1	Por defecto, un conector DBR Twitter realiza una iteración por minuto para obtener los nuevos posibles tweets. En cada iteración se produce una petición para obtener Mensajes directos, una para obtener menciones y una para los resultados de búsqueda.	El número máximo de tweets obtenidos por iteración es de 200 para mensajes directos, 200 para menciones y 100 para búsquedas.
2	Limitaciones de uso de Twitter API en Mensajes directos y menciones.	Según documentación de https://dev.twitter.com/docs/rate-limiting/1.1/limits acerca del Rate Limiting, el número máximo de peticiones autenticadas del tipo 'DM' es de 15 cada 15 minutos de igual manera que el de tipo 'Mention'. Estas peticiones son medidas respecto al token de autenticación que realiza la petición.
3	Limitaciones de uso de Twitter API en búsquedas.	Según documentación de https://dev.twitter.com/docs/rate-limiting/1.1/limits acerca del Rate Limiting, el número máximo de peticiones no autenticadas (del tipo 'search') permitidas es de 180 cada 15 minutos. Estas peticiones son medidas respecto al token de autenticación que realiza la petición.

4	Algunos consejos para realizar búsquedas en Twitter. Mas información en http://support.twitter.com/articles/344721-como-usar-operadores-de-busqueda-avanzada-en-twitter	- En la medida de lo posible, hacer uso de la interfaz de Búsqueda avanzada de Twitter para generar la sentencia de búsqueda y copiar y pegar en la URL del conector. - Las busquedas a través de Twitter Search API entregan tanto tweets como retweets. Si se quisieran descartar los retweets de los resultados de la búsqueda, se podría hacer indicando "*exclude:retweets*" a través de la propia cadena de texto a buscar. - Si se quiere acotar el resultado de la busqueda a aquellos tweets que estén escritos en un idioma determinado se puede hacer indicando p.e. "*lang:es*" en la cadena de texto a buscar.

18.5 COMO CODIFICAR CARACTERES ESPECIALES EN LAS DEFINICIONES DE CONECTORES (URL)

El formato de configuración de un conector (URL) se especifica según:

Protocol://[UserInf@][[Host]:[Port]][/[Ruta][?[[ParamN]=[ValueN]]&…]]

En determinados casos puede ser necesario codificar alguna de las partes que forman dicha URL, para evitar que contengan caracteres inadecuados.

Por ejemplo, algunos servidores email POP3 requieren especificar un dominio en el nombre de usuario. Ejemplo:

```
usuario@dominio.com
```

En estos casos, cuando se escribe la URL correspondiente a un conector email POP3 DBR, el carácter @ deberá codificarse según las normas estándar de URLs

Así en el ejemplo anterior deberá codificarse "usuario@dominio.com" como "usuario%40dominio.com", y por tanto la URL de conector POP3 DBR sería:

```
pop3://usuario%40dominio.com:password@mail.dominio.com
```

De forma equivalente, si otros campos (p.ej: el campo password o servidor) contuviesen algún otro carácter inadecuado según las reglas de codificación URL, también deberían codificarse.

Ejemplo:

usuario: 'usuario@dominio.com'

password = 'pwd 10' (notar que contiene un espacio en blanco)

```
pop3://usuario%40dominio.com:pwd%2010@mail.dominio.com
```

Caracteres reservados

!	#	$	&	'	(	)	*	+	,	/	:	;	=	?	@	[	]
%21	%23	%24	%26	%27	%28	%29	%2A	%2B	%2C	%2F	%3A	%3B	%3D	%3F	%40	%5B	%5D

Referencias:

http://en.wikipedia.org/wiki/Percent-encoding

http://www.ietf.org/rfc/rfc1738.txt

19 ANEXO D: INSTALACIÓN EN UN 'CLUSTER FAILOVER' DE WINDOWS 2008

Si dispone de un 'cluster failover' de Windows 2008 puede configurar un servicio Evolution de alta diponibilidad siguiendo las indicaciones que vienen a continuación.

19.1 REQUERIMIENTOS

Un 'cluster failover' sobre Windows 2008 en funcionamiento[4].

Una unidad de almacenamiento[5] para el 'Servicio Evolution de alta disponibilidad' que se configurará en el cluster y que deberá estar identificada por la misma unidad en los nodos del cluster.

Los nodos del Cluster han de tener un **hardware idéntico**.

19.2 INSTALACIÓN DEL SERVIDOR EVOLUTION

La instalación de un servidor Evolution está descrita en el apartado (6) del manual, aunque existen ligeras diferencias que se comentan a continuación.

1	Microsoft Internet Information Server (6.2.2) debe instalarse en cada nodo.
2	El servidor CTI (6.2.3) debe instalarse en cada nodo.
3	A continuación debe seguir los pasos de instalación de Evolution (6.3) en cada nodo.
4	Al finalizar la instalación se deberá copiar el archivo que se encuentra en la carpeta de instalación de Evolution *Evolution\Server\addons\Clusweb7.vbs* a la carpeta de Windows *System32\InetSrv.*
5	La configuración (6.4) sólo la deberá realizar en uno de los nodos.
6	La introducción de la licencia (6.5) se hará más adelante.

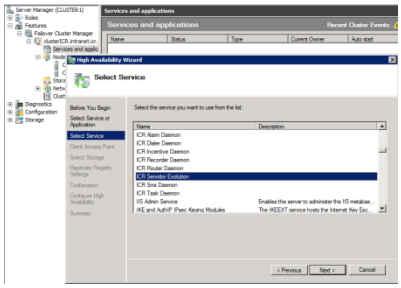
[4] Si necesitan configurar el Cluster pueden seguir esta guía de Microsoft:
Failover Cluster Step-by-Step Guide: Configuring a Two-Node File Server Failover Cluster

[5] En dicha unidad se almacenará la configuración compartida de los IIS, las aplicaciones WEB de Evolution (incluidos los argumentarios desplegados) y las grabaciones de Audio.

19.3 CONFIGURACIÓN DEL 'SERVICIO DE ALTA DISPONIBILIDAD DE EVOLUTION'

A continuación crearemos el 'Servicio de alta disponibilidad' e incluiremos los elementos necesarios para que Evolution se ejecute desde uno de los nodos.

1 Configure un nuevo 'servicio de alta disponibilidad' llamado **EvoCluster**, a partir de la plantilla de servicio genérico ICR Evolution Server, en el nodo donde haya configurado Evolution.



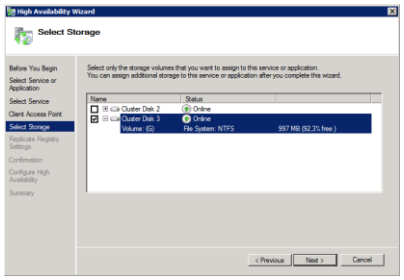
2 Incorpore las ramas del registro de windows:

[HKLM]\Software\Activa

Windows 2008 x86:
[HKLM]\Software\ICR

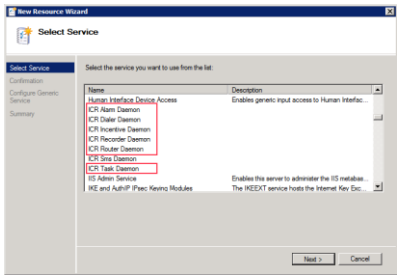
Windows 2008 x64:
[HKLM]\Software\Wow6432Node\ICR
[HKLM]\Software\ICR

3 Incorpore la unidad de almacenamiento compartida entre los clusters.

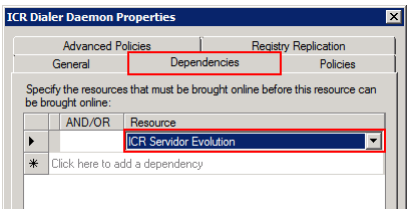


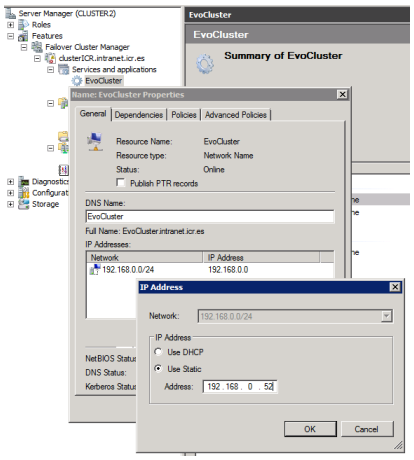
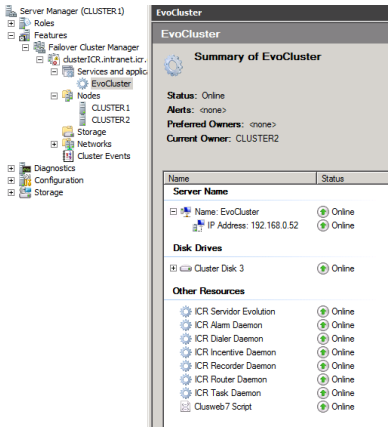
4 Incorpore los servicios ICR:

ICR Dialer Daemon
ICR Incentive Daemon
ICR Recorder Daemon
ICR Router Daemon
ICR Task Daemon



5 A cada uno de estos servicios hay que incorporarle una dependencia (Propiedades → Dependencias) de "ICR Servidor Evolution".



6	Incorpore el script *Clusweb7.vbs* de la carpeta de Windows *System32\InetSrv.*	
7	Asigne una IP estática al 'servicio de alta disponibilidad' creado. *EvoCluster → Propiedades → General → Red*	
8	Reinicie el servicio EvoServer.	
9	Introducción de licencias de Evolution.	Siga las indicaciones del apartado (6.5)

19.4 CONFIGURACIÓN COMPARTIDA DE LOS IIS

Extraído del artículo de Microsoft: Configuring IIS 7.0 World Wide Web Publishing Service in a Microsoft Windows Server 2008 failover cluster

1	Cree una carpeta en la unidad compartida para guardar la configuración compartida de los IIS.
2	Cree un usuario con permisos de control total en la carpeta anterior.
3	Cree una carpeta en la unidad compartida para guardar las aplicaciones web de Evolution.
4	En cada nodo: 1. Abra un símbolo del sistema administrativo. 2. Ejecute el comando siguiente: **net stop apphostsvc** 3. Ejecute el comando siguiente: **sc privs apphostsvc** **SeChangeNotifyPrivilege/SeTcbPrivilege/SeImpersonatePrivilege** 4. Ejecute el comando siguiente: **net start apphostsvc**
5	En uno de los nodos del clúster, exportar la configuración compartida para el recurso compartido de archivos: 1. Vaya a **Herramientas administrativas** y, a continuación, haga clic en **Administrador de servicios de Internet Information Server (IIS)**. 2. En el panel izquierdo, haga clic en el nodo de nombre de servidor. 3. Haga doble clic en el icono de **Configuración compartida**. 4. En la página Configuración compartida, haga clic en **Exportar configuración** en el panel de **acciones** (panel derecho) para exportar los archivos de configuración desde el equipo local a otra ubicación. 5. En el cuadro de diálogo **Exportar configuración**, escriba la ruta de acceso del recurso compartido de archivos en el cuadro **ruta de acceso física**. 6. Haga clic en **Conectar como** y, a continuación, escriba el nombre de usuario y la contraseña para la cuenta de usuario que tiene acceso al recurso compartido en el que se almacena la configuración compartida y, a continuación, haga clic en **Aceptar**. Esta cuenta se utilizará para tener acceso al recurso compartido. Debe utilizar una cuenta de Active Directory

restringida que no es el administrador del dominio.

7. En el cuadro de diálogo **Exportar configuración**, escriba una contraseña que se va a utilizar para proteger las claves de cifrado y, a continuación, haga clic en **Aceptar**.
8. En la página de **Configuración compartido**, haga clic para seleccionar la casilla de verificación **Habilitar configuración compartida**.
9. Escriba la ruta de acceso física, la cuenta de usuario y la contraseña que escribió anteriormente y, a continuación, haga clic en **aplicar** en el panel de **acciones**.
10. En el cuadro de diálogo **Contraseña de claves de cifrado**, escriba la contraseña de clave de cifrado que establezca anteriormente y, a continuación, haga clic en **Aceptar**.
11. En el cuadro de diálogo **Configuración compartida**, haga clic en **Aceptar**.

---

6 En cada uno de los otros nodos del clúster, utilice la configuración compartida que acaba de exportar el recurso compartido de archivos:

1. Vaya a **Herramientas administrativas** y, a continuación, haga clic en **Administrador de servicios de Internet Information Server (IIS)**.
2. Haga clic en el nodo de nombre de servidor.
3. Haga doble clic en el icono de **Configuración compartida**.
4. En la página de **Configuración compartido**, haga clic para seleccionar la casilla de verificación **Habilitar configuración compartida**.
5. Escriba la ruta de acceso física del recurso compartido de archivos, la cuenta de usuario y la contraseña escrita previamente y, a continuación, haga clic en **aplicar** en el panel de **acciones**.
6. En el cuadro de diálogo **Contraseña de claves de cifrado**, escriba la contraseña de clave de cifrado que establezca anteriormente y, a continuación, haga clic en **Aceptar**.
7. En el cuadro de diálogo **Configuración compartida**, haga clic en **Aceptar**.

---

7 Mueva las aplicaciones Web: Manager, Webroot, ScriptServer y Scripts/* a la unidad compartida.

1. Copie las carpetas Manager, Webroot y Evolution a la unidad compartida donde sea accesible por los IIS.
2. De permisos de control total a 'todos' en las carpetas Logs y Audio de Manager.
3. De permisos de control total a 'todos' en las carpetas Logs de ScriptServer y Scripts/*.
4. Elimine de todos los nodos las **aplicaciones Web**: Manager, NCROOT, ScriptServer, DeveloperService, Scripts/*.
5. Elimine de todos los nodos las **carpetas** Manager, Webroot y Evolution.
6. Cree en el nodo activo las aplicaciones Web: Manager, ScriptServer y Scripts/*, asociadas al grupo de aplicaciones **Evolution.**
7. Cree en el mismo nodo la aplicación Web: NCROOT asociada al grupo de aplicaciones por **defecto.**
8. Cree en el mismo nodo la aplicación DeveloperService asociada al grupo de aplicaciones **EvolutionDeveloperService.**